# PRESIDENTIAL PRIVACY INITIATIVE

July 21, 1978

DRAFT

Approved For Release 2003/04/17 : CIA-RDP81-00142R000700030005-0

recd 26 July

**UNITED STATES DEPARTMENT OF COMMERCE**
**National Telecommunications and Information Administration**
Washington, D.C. 20230

July 21, 1978

MEMORANDUM FOR: PRIVACY POLICY
COORDINATING COMMITTEE

FROM: HENRY GELLER (Assistant Secretary of Commerce for Communications and Information)

RICK NEUSTADT (Assistant Director, Domestic Policy Staff)

We are submitting the Response Memorandum for this study. This Memorandum is based on the report of the Privacy Protection Study Commission and on the agencies' reactions, as indicated in the reports of the six task forces. The Memorandum was prepared by the Privacy Initiative staff at the National Telecommunications and Information Administration, Department of Commerce, under the direction of Arthur Bushkin.

This Memorandum needs your review and discussion before a decision memo can go to the President. We would like your written comments on these questions:

(1) Does this paper inaccurately state your position on any issue?

(2) Do you have any serious objections to any of the items reported as "areas of agreement"? (Silence will be taken as indicating agreement.)

(3) For each issue of concern to you in the "areas of disagreement" or "issues for decision" sections, which option do you recommend (including an option that has not been listed, if appropriate)?

(4) Should any privacy issues be addressed which are not currently discussed?

(5) Which issues appear amenable to resolution through further interagency coordination, without need for Presidential decision?

(6) Which issues do you believe require Presidential decision?

The comments should be submitted by August 14. (We have set this deadline because the agencies have already studied the issues in preparing the task force reports, so further extensive study should not be necessary.) Please send one copy to Rick Neustadt (Room 208, Old Executive Office Building, Washington, DC 20500) and five copies to Art Bushkin (Room 706, 1800 G Street, NW, Washington, DC 20504; tel. 395-3122)

This Memorandum presents preliminary, tentative views and is circulated only for discussion purposes. No part of it -- including the items labelled "areas of agreement" -- purports to state the Administration's position.

Please do not circulate this Memorandum outside of your agency.

Attachment

cc: other interested agencies.

# Presidential Privacy Initiative

July 21, 1978

Draft

## Preface

In July, 1977, the Privacy Protection Study Commission delivered its final report to the President and the Congress. The Administration's response to that report has been coordinated under the Domestic Policy Review System.

A Cabinet-level Coordinating Committee was established, and the Commission's report divided into six areas and assigned to task groups for analysis and response. This document distills the task group reports. While alternatives to the Commission's recommendations were considered, this effort was fundamentally a response to the Commission's report. It was not an independent analysis of the privacy problem.

The Presidential decision package is currently planned to have two parts:

1. a brief Presidential Review Memorandum highlighting the issues for Presidential decision; and

2. a supporting document containing a more complete discussion of the issues and options.

This document is the latter.

This particular draft is part of a deliberative policy-making process and is an internal government working paper. It is not intended for public release. It has not been reviewed by the agencies to verify that their positions are accurately represented, and it does not represent the policy of the Administration.

TABLE OF CONTENTS

Approved For Release 2003/04/17 : CIA-RDP81-00142R000700030005-0

# I. Introduction

## A. Structure of This Document

This document is divided into six parts. The first is a detailed introduction and the last five present a number of basic privacy policy issues for decision. In most cases, the issues can be decided as if they were independent of one another in that a particular decision on one issue need not force a related decision on another issue. As Section I.G. suggests, however, a comprehensive privacy policy is usually understood to have certain essential elements.

Part I provides the historical background and analytical framework for the document, and sets out the basic elements of a privacy policy. These elements, such as an individual's right to see and copy the records maintained about him, and to have a means of challenging records he thinks are inaccurate, are offered as the basis for an Administration privacy policy. The privacy policy under consideration is not meant to apply to all records or record-keeping relationships. Specific decisions concerning the way these elements might be applied to specific kinds of organizations are set out in Parts II through VI. The subsequent discussion includes specific limits on scope and coverage. No inferences should be drawn regarding extension of any policy beyond the areas presented below.

Part II contains a description of nine different industries or types of records for which the Privacy Protection Study Commission recommended privacy protections. Following the description of each industry are the decisions, including a discussion of the various options, concerning application of the basic privacy policy to that industry.

Part III deals with government access to records maintained by the private sector and by state and local governments. It primarily concerns access by law enforcement and regulatory agencies.

Part IV discusses two areas concerning Federal record-keeping activity. The first is revision of the Privacy Act of 1974, and the second deals with government operation of electronic funds transfer services for private sector organizations.

Part V contains three cross-cutting topics: the use of truth verification devices, such as lie detectors;

the establishment of a standard personal identifier; and the protections necessary to allow use of Federally maintained or financed records about individuals for research and statistical purposes.

Part VI deals with the establishment of new or expanded privacy-related functions to be performed by the Federal government.

Finally, the Appendix lists seriatim all of the decisions that have been presented throughout the document.

B. Information Privacy

This memorandum presents the policy choices underlying a potential Administration position on privacy. The use of the term "privacy" in this context, however, is somewhat ambiguous. A more appropriate phrase would be record-keeping privacy or, as it is more commonly called, information privacy, for what is being discussed is the collection, maintenance, use, and dissemination of information about people.

The term "privacy," as it applies to recorded information, does not mean simply "confidentiality," "secrecy," or "limits to disclosure." In this context, "privacy" or "information privacy" also embodies notions of fairness, or more precisely, fair information practice. Indeed, privacy statutes of the type discussed herein are often called fair information practice statutes. (In other countries, they are called data protection statutes.)

While no precise definitions of "privacy," "fairness," or "fair information practice" exist, these concepts are generally understood in this context to mean providing individuals with procedural rights and mechanisms by which they may hold record-keeping organizations accountable for their record-keeping practices. One such procedural right, or fair information practice protection, for example, is that individuals be able to see and obtain a copy of the information about them which is maintained by a record-keeping organization. The goal of these individual rights is often described as giving the individual some measure of control over information about himself, although the term "control" is obviously too strong a concept. In fact, information privacy also recognizes an organization's interest in the content of a record and tries to capitalize on that interest in establishing protections for the individual. Basically, information privacy is an emerging body of procedural law, with only a few instances of substantive standards (e.g., the Privacy Act's prohibitions on the collection of information relating to an individual's exercise of his First Amendment rights).

The developing body of law in the area of information privacy is only loosely related to other, more conventional aspects of privacy law. The common law tort of privacy invasion is generally divided into four categories: (1) intrusion upon an individual's physical solitude or seclusion; (2) public disclosure of private facts about an individual; (3) publicity which places an individual in a false light in the public eye; and

(4) appropriation of an individual's name or likeness. By and large, the courts have refused to apply any of these four categories where organizational record-keeping practices have been at issue, and this is one major reason why new public policy is needed.

Generally speaking, the first and second categories relate most closely to information privacy. The remedies, however, of the tort theory center around the collection of damages after an injury. Information privacy, on the other hand, attempts to establish, through a system of checks and balances, an environment in which the chance of injury occurring is minimized. Moreover, information privacy establishes a broader set of individual rights and organizational responsibilities in that it focuses not just on the disclosure of information, but on an organization's collection, maintenance, and use of information as well.

For the remainder of this memorandum, unless otherwise noted, the term "privacy" will be used to mean only "information privacy." This excludes other, more conventional privacy issues, such as surveillance, wiretapping, sexual freedom, and intrusions into the home, except to the extent that they relate to a record keeper's information practices.

C. Statement of the Problem

The privacy legislation to date, most of which has been fairly recent, represents a varied and sometimes inconsistent attempt to address a problem the precise nature of which is still emerging. Over the past decade, there has been an increasing awareness that the misuse of recorded information could be the source of harm or unfairness to individuals. More recently has come the realization that the well-intentioned use of recorded information could also have undesirable consequences. Furthermore, while recorded information increasingly mediates relationships between people and organizations, individuals have less and less control over these records. And contributing to this trend has been the explosion of information technology, particularly in computers and telecommunications, which not only magnifies the problems of manual systems, but also introduce some new problems as well (e.g., the accumulation of personal information in electronic funds transfer systems).

American life has changed dramatically in this century, particularly in the last three decades. Most Americans now do at least some of their buying on credit, and most have some form of life, health, property, or liability insurance. Institutionalized medical care is almost universally available. Government social services programs now reach deep into the population, as do government licensing of occupations and professions, Federal taxation of individuals, and government regulation of business and labor union affairs. Today, the government regulates and supports large areas of economic and social life through some of the nation's largest bureaucratic organizations, many of which deal directly with individuals.

A significant consequence of this marked change in the variety and concentration of institutional relationships with individuals is that record keeping about individuals now affects almost everyone. People have their credit-worthiness evaluated on the basis of recorded information in the files of one or more organizations. The same is true for those seeking insurance, medical care, employment, education, and social services. Each of these relationships requires the individual to divulge information about himself, and usually leads to some evaluation of him based on personal information that some other record keeper has compiled. In short, we live, inescapably, in an "information society," and few of us have the option of avoiding relationships with record-keeping organizations. To do so is to

forego not only credit but also insurance, employment, medical care, education, and all forms of government services to individuals.

The increased use of computers in such record-keeping activities tends to eliminate the pattern of informal protections for the privacy of personal information which existed when it took a great deal of time and cost a good bit of money to process or retrieve recorded information. Furthermore, the growing availability and decreasing cost of computer and telecommunications technologies provide both the impetus and means to perform new record-keeping functions. And the pace of technological development will only accelerate this trend in the future.

Coupled with this disappearance of the informal protections which promoted the proper use and confidentiality of recorded personal information, is the fact that formal, legal protections for personal records are in many cases nonexistent. When our existing legal structure was developed, most information of an intimate or revealing nature, such as financial records, was in the exclusive control and possession of the individual. Thus, the laws protecting personal information, like the Fourth and Fifth Amendments to the Constitution, were designed to protect information in the actual possession of the citizen.

Today, a good deal of an individual's personal information is relinquished to organizations, governments included, which demand it in order to provide essential services; however, little legal protection has been extended to these records. As a result, the individual lacks protections against others obtaining and using financial, medical, and similar personal data about him. In addition, in this age of giant organizations, the individual does not possess the bargaining power in the marketplace to fashion protections for how organizations will use and disclose his records. At the same time, the citizen has lost the reality of his constitutional protections against the biggest organization of all--government. That intimate personal information that the Fourth and Fifth Amendments were designed to protect is open to largely unaccountable government examination and is even demanded, as a matter of course, by the government from record keepers on whole classes of citizens.

The Privacy Protection Study Commission concluded that since so much of an individual's life is now shaped

by his relationships with organizations, his interest in the records organizations keep about him is obvious and compelling. The Commission further concluded that, if the individual's interest is to be protected, public policy must focus on five sytemic features of personal-data record keeping in America today.

1. While an organization makes and keeps records about individuals to facilitate relationships with those individuals, it also makes and keeps records about individuals for other purposes, such as documenting the record-keeping organization's own actions, thus making it possible for other organizations--government agencies, for example- to monitor the actions of individuals.

2. There is an accelerating trend, most obvious in the credit and financial areas, toward the accumulation in records of more and more personal details about an individual.

3. More and more records about an individual are collected, maintained, and disclosed by organizations with which the individual has no direct relationship but whose records help to shape his life.

4. Most record-keeping organizations consult the records of other organizations to verify the information they obtain from an individual and thus pay as much or more attention to what other organizations report about the individual than they pay to what he reports about himself; and

5. Neither law not technology now gives an individual the tools he needs to protect his legitimate interests in the records organizations keep about him.

The significance of this view of the problem is that it focuses on systemic characteristics of our society rather than on specific record-keeping abuses. This was a major policy decision of the Privacy Commission, and it is a view shared by many who are familiar with the trends in both record keeping and the law.

The view that societal trends rather than specific abuses are the driving force for action draws attention to the fact that the forces which are undermining personal privacy often operate slowly and subtlely. The Commission

concluded, for example, that

> the problems perceived by the Congress at the time of the Privacy Act's passage have turned out to be more complex than anticipated, and by and large they are independent of the problem of premediated abuse... The real danger is the gradual erosion of individual liberties through the automation, integration, and interconnection of many small, separate record-keeping systems, each of which alone may seem innocuous, even benvolent, and wholly justifiable. (Commission emphasis)

Thus, the Privacy Commission and other experts warn that we are faced with a slow but steady erosion of privacy which, if left unreversed, will take us in another generation to a position where the extent of our human rights and the vitality of our democracy will be jeopardized.

This view is not, of course, universally shared. Organizations which might be covered by privacy protection point to the "lack of documented abuse." One problem is that abuses in this area are often difficult to document, although numerous abuses have been documented by the Commission and various legislative bodies. The basic public policy choice, however, is whether the measures described herein are, or should be, directed at specific abuses or whether the trend of affairs is such that the proposed protections are required as a result of a fundamental value choice about the nature of our society.

Interestingly, many private sector organizations that oppose privacy protection legislation do so on the basis of cost or opposition to government regulation. Yet, these same organizations are often quite willing to implement privacy safeguards, usually along the lines suggested by the Privacy Commission, on a voluntary basis. There is, in short, a broader consensus on the nature of the problem (i.e., that the role of the individual needs to be strengthened vis a vis law, technology, and record keeping) than there is on the nature of the proposed solution, although even this is slowly changing in the year since the Commission's report was published.

Finally, any attempt to resolve the privacy problem must balance the goals of privacy protection with other significant competing public interests. If they are to operate effectively, business, government, and other

institutions have legitimate needs to collect, use, and disclose information about individuals. If the concern for privacy were taken as an absolute, the ability of government, for example, and particularly law enforcement, to perform its required duties could be severely constrained.

Other less tangible values may also conflict with the objective of personal privacy -- or at least the way one chooses to go about preserving it. Beginning with the First Amendment protections of freedom of speech and freedom of the press and continuing with the more recent drives for open government, our society has continuously affirmed its concern for the free flow of information. To the extent that privacy protections involve restraints on the free flow of information about individuals, the values of privacy and the values of free speech have to be carefully balanced. Equally important are concerns about too great an intrusion by government into private affairs in order to preserve what many view essentially as private interests -- particularly when the greatest actual and potential offender against rights of privacy has been the government itself. Thus, the choices in the area of privacy are generally not between "good" and "evil," but between legitimate, though competing, public interests.

D. Legislative History

Privacy protections have a long history in this country, emanating from the Fourth Amendment's prohibition of unreasonable searches and siezures. In recent years, a fairly consistent body of information privacy principles has appeared in a number of Federal statutes and in the reports of several Federal study commissions.

These principles had their beginning in the "Code of Fair Information Practices" contained in 1973 report of the DHEW Secretary's Committee on Automated Personal Data Systems, and had their fullest and most explicit legislative expression as the eight principles of the Privacy Act of 1974:

(1) There shall be no personal-data record-keeping system whose very existence is secret and there shall be a policy of openness about an organization's personal-data record-keeping policies, practices, and systems. (The Openness Principle)

(2) An individual about whom information is maintained by a record-keeping organization in individually identifiable form shall have a right to see and copy that information. (The Individual Access Principle)

(3) An individual about whom information is maintained by a record-keeping organization shall have a right to correct or amend the substance of that information. (The Individual Participation Principle)

(4) There shall be limits on the types of information an organization may collect about an individual, as well as certain requirements with respect to the manner in which it collects such information. (The Collection Limitation Principle)

(5) There shall be limits on the internal uses of information about an individual within a record-keeping organization. (The Use Limitation Principle)

(6) There shall be limits on the external disclosures of information about an individual a record-keeping organization may make. (The Disclosure Limitation Principle)

(7) A record-keeping organization shall bear an affirmative responsibility for establishing reasonable and proper information management policies and practices which assure that its collection, maintenance, use, and dissemination of information about an individual is necessary and lawful and that the information itself is current and accurate. (The Information Management Principle)

(8) A record-keeping organization shall be accountable for its personal-data record-keeping policies, practices, and systems. (The Accountability Principle)

Some or all of these principles are applied, in different forms, to specific kinds of records, record keepers, and record-keeping practices by a number of Federal statutes. Including the Privacy Act, the foremost of these statutes are:

a. Freedom of Information Act--Enacted in 1966 and amended in 1974, this statute requires the disclosure, subject to certain exceptions, of substantive and policy information maintained by Federal agencies to any person. As a result of this right of access, individuals are also able to obtain access to records about themselves, and thus, to a limited extent, this act and the more recent Privacy Act of 1974 overlap.

b. Privacy Act of 1974--Enacted in 1974, this statute is Congress' first attempt to incorporate comprehensive privacy protections into the records management practices of the Federal government. The act regulates the collection, maintenance, use, and disclosure of personal information in the Federal sector. Except for certain government contractors, it does not apply to the private sector. Basically, it requires public notice of agency record systems, provides for individual access to personal records, sets up procedures for an individual to correct or amend records about himself, limits disclosures of records, and establishes certain practices and policies of fair information practice. Individual access to the Federal district courts is available for enforcement purposes, and provision is made for both civil remedies and criminal penalties.

c. Fair Credit Reporting Act--Enacted in 1970, this statute applies only to consumer-reporting agencies, i.e., entities that supply credit history and individual

background information to credit grantors, insurers, employers, and others. The intent of the act is to enable a consumer to learn the "nature and substance" of all information pertaining to him in the records of a consumer-reporting agency, and to learn when a consumer report adversely affects a decision about him. The consumer may also demand a reinvestigation of the material and deletion or amendment of inaccurate or unverifiable information. The act places some loose disclosure limitations on a consumer-reporting agency. Individuals may recover civil damages in Federal or state courts and criminal penalties are provided. The FTC has primary enforcement authority under this act, along with other regulators of financial institutions.

d. Family Educational Rights and Privacy Act--This statute, better known as the "Buckley-Pell Amendments," was enacted and amended in 1974. It provides for access by students over 18 or parents of minor students to all "education records" maintained by any educational institution receiving Federal funds. Also, the act sets rather stringent limits on the disclosure of such records to third parties which may be made without parental or student consent. The requirements of the act are enforceable by the Secretary of the DHEW, whose only enforcement mechanism is the denial of Federal funds to any offending institution. DHEW also has the responsibility to issue regulations to be followed by educational institutions.

e. Equal Credit Opportunity Act--Enacted in 1974, and amended in 1976, this act proscribes discrimination in the granting of credit on nine bases, including race, religion, national origin, sex, marital status, and age. Although the collection of such information about credit applicants is often necessary to demonstrate compliance with the law, the use of such information about credit applicants is strictly limited. The basis for any denial of credit must be provided in writing. An individual can bring suit in Federal or state court to enforce the act, and can receive both money damages and equitable relief. Administrative enforcement rests with the Federal Trade Commission and with a number of other Federal agencies, primarily financial institution regulators.

f. Fair Credit Billing Act--Enacted in 1974, this statute was amended in 1976. It basically regulates the use of information about a credit card holder by his creditor when a dispute develops between those

parties as to the amount owed. It permits a debtor to challenge and correct erroneous billing information and prohibits dissemination of adverse credit reports until the dispute is resolved. Enforcement is essentially the same as the Equal Credit Opportunity Act.

g. Fair Debt Collection Practices Act--Enacted in 1977, this statute regulates debt collectors, and is designed to prevent abusive, deceptive, and unfair debt collection practices. Of particular interest to privacy, it prohibits various kinds of pretext interviews and other false representations of the debt collector's identity or business affiliation. It also prohibits communicating with the consumer's employer or other third parties about his debts, or publishing lists of alleged debtors, other than through a consumer reporting agency.

There are also numerous Federal statutes which have privacy implications because they require organizations to collect, maintain, or disclose certain records. One example is the Bank Secrecy Act, enacted in 1970, which, despite its title, is not a "secrecy" act. Rather, it requires banking institutions to report to the Secretary of the Treasury information on certain types of financial transactions. It also requires banks to maintain certain records, including checks, for five years. Civil and criminal penalties are available against offending banking institutions. The Department of the Treasury has the responsibility to issue regulations under this act.

The whole issue of privacy as that concept pertains to personal banking records has also been seriously affected by the recent Supreme Court case of United States v. Miller, 425 U.S. 435 (1976). In that case, the Court held that a private individual has no legitimate "expectation of privacy" in his bank records and thus no legally enforceable interest for courts to consider. The Court ruled that checks negotiated by the individual are an independent record of that person's participation in the flow of commerce and, as such, are not to be considered confidential communications. Moreover, the court ruled that the bank records do not belong to the individual, but to the banking institution.

E. The Privacy Protection Study Commission

There have been a number of distinguished study efforts addressing the privacy problem. Most notable among those which preceeded the Privacy Commission were:

- The DHEW Secretary's Advisory Committee on Automated Personal Data Systems. -- This 1973 report first presented the principles of a "Code of Fair Information Practice," and is generally credited with providing the intellectual framework for the Privacy Act of 1974.

- The Domestic Council Committee on the Right to Privacy. -- During its life (1974-1976), this group brought high level visibility to the privacy issue and direct involvement by the Executive Office of the President.

Motivated by the work of these two committees and the work of various congressional committees, the Congress and the Executive Branch worked together to enact the Privacy Act of 1974. That act stands as the most concerted effort to date to resolve information privacy issues and to protect the interests of individuals in connection with records about them maintained by others. The Privacy Act, however, is aimed exclusively at Federal records and Federal record keepers. The concern remained that the problems of privacy protection were not limited to Federal records. Consequently, Congress decided that there should be further study to determine if the principles and requirements of the Privacy Act of 1974 should be applied to private sector record keepers and to state and local governments.

Addressing these questions was the basic charge to the Privacy Protection Study Commission, a two-year independent Federal commission created by the Privacy Act. The Privacy Commission was given a broad mandate to: (1) investigate the personal information record-keeping practices of governmental, regional, and private organizations and to recommend to the President and the Congress the extent, if any, to which the principles and requirements of the Privacy Act should be extended to such organizations; and (2) make any other recommendations necessary to protect the privacy of individuals while meeting the legitimate needs of government and society for information. In July 1977, the Privacy Commission responded to its mandate with a 654-page report containing

162 specific recommendations, and numerous less emphatic suggestions, supporting broader extension of the principles of the Privacy Act, but not the Act's specific requirements.

In recommending extension of the principles, but not the requirements, of the Privacy Act to the non-Federal sector, the Privacy Commission made some explicit and implicit decisions regarding the applicability and appropriateness of these principles beyond the Federal sector. For example, the Commission determined that the Privacy Act's principle that there should be no secret record systems cannot be extended, not because it is not a desirable objective, but rather because there is no realistic mechanism for implementation. (In the Federal sector, notices describing agency record systems are published in the Federal Register.) Thus, while the fundamental objectives remain the same, the basic elements of a privacy policy in the non-Federal sector would differ from the Privacy Act principles.

The Privacy Commission also rejected the omnibus approach of the Privacy Act as being inappropriate for the non-Federal Sector. The Commission recommended instead that non-Federal privacy protection legislation be enacted on an industry-by-industry basis (e.g., banking, credit, insurance) or on a community-by-community basis (e.g., medical, education, social service and public assistance). In this way, the specific characteristics and requirements of each industry or community could be considered.

The Privacy Commission's recommendations have the same general thrust as those of its predecessors. Driven by findings of actual and potential misuse of personal records, as well as by a concern for the gradual erosion of personal privacy resulting from the well-intentioned use of modern information technology, several Congressional committees, the DHEW Advisory Committee, the Domestic Council Committee on the Right to Privacy, and the Privacy Commission have all concluded that the way in which records about individuals are collected, maintained, used, and disclosed has to be changed. In particular, all the groups examining the problem have called for some degree of control of personal records to be returned to the individuals to whom those records pertain.

These groups have urged the creation or bolstering of mechanisms to limit the collection of information by organizations. They have suggested specific restrictions on the gathering of information by government. They

have consistently recommended that an individual be provided the right to see and obtain a copy of records about himself, to correct errors in those records, and to be informed of (and, in some cases, limit) the uses to which those records will be put. And, they have endorsed the creation of a right for the individual to exercise some measure of control over the disclosure of records about himself outside the organization maintaining them.

The Privacy Commission's recommendations have three basic objectives: minimizing intrusiveness, maximizing fairness, and creating legitimate expectations of confidentiality. The goal of mimimizing intrusiveness is to limit the collection of unnecessary or offensive personal information by organizations. The objective of maximizing fairness is to open up the process by which organizations use records about individuals, to permit the individual to know what is being done with personal information, and to allow him to ensure its accuracy and proper use. The creation of "legitimate expectations of confidentiality" is an effort to give legal recognition to the personal character of records about an individual and to establish a legitimate interest for the individual in what happens to those records. Such a legal interest would have two parts: (1) placing a duty on a private sector record keeper not to disclose recorded information about an individual without his authorization or consent; and (2) limiting the government's access to records held by private sector record keepers by requiring government to use legal process to obtain such records.

In addition, the Commission concluded that giving rights and responsibilities to individuals and the organizations with whom they dealt was not enough. In order to monitor industry-wide activities, to be able to respond to the unforeseen consequences of the growth of information technology, and, in particular, to structure and enforce privacy policy effectively within the Federal government, the Commission recommended both that existing regulatory authority be augumented and that a new government entity be created. This combination, the Commission believed, was essential to ensure that personal privacy, and the basic values of individuality which underlie it, would continue to be protected in American society.

F. Current Activity

Congressional

Since the Privacy Commission issued its report there has been a great deal of privacy interest in Congress. Immediately upon submission of the report, Congressmen Koch and Goldwater (both members of the Privacy Commission) introduced about a dozen bills that substantially followed the Commission's recommendations. Congressman Preyor reintroduced all of these bills as one omnibus bill, H.R. 10076. Congressman Preyor's Subcommitee on Government Information and Individual Rights recently has held hearings on this bill.

Only a few issues, however, are the focus of legislative activity this term. First is the issue of government access to financial records. The House Banking Committee (H.R. 13088) and Judiciary Committee (H.R. 214) are considering similar bills that generally follow the Commission's approach. The Senate is also considering similar legislation. The Departments of Justice and the Treasury have already presented their own views on this legislation to both Senate and House committees.

Second, provisions protecting the privacy of financial records generated by electronic fund transfer (EFT) systems are included in legislation recently reported out of the Senate Banking Committee. Third, medical record privacy was raised during the first session of this term in the context of amendment of the Social Security Act. Action on the proposed medical record privacy sections was tabled in committee until DHEW had time to develop a position in response to the Commission's report. In May 1978, DHEW presented its own views to the Congress.

State

Activity in privacy matters resulting from the Privacy Commission's report is not limited to the United States Congress, nor is the Federal government in the lead in developing updated privacy protection. A number of states, led by California, have developed significantly greater privacy protections than are afforded by Federal law. Nine states now have constitutional provisions protecting individual privacy; seven states have passed omnibus privacy statutes similar to the Federal Privacy Act; eleven states have passed statutes that go beyond

the Federal Fair Credit Reporting Act; sixteen states have laws governing the disclosure of personal information by financial institutions; some states regulate the personal information practices of private sector employers; and many states have laws governing medical records. And this activity is expected to increase. This proliferation of state legislation has engendered some business support for Federal legislation that would provide uniformity of treatment for enterprises that operate nationwide.

International

There is also an international dimension to the privacy issue. The locus of this emerging activity is Western Europe. In 1973, Sweden became the first European country to pass privacy protection legislation. Within the last 12 months, West Germany, France, Norway, and Denmark have adopted national legislation dealing with privacy protection. Other European countries and Australia are actively considering such legislation, and Canada, with a statute similar in some respects to the U.S. Privacy Act, is also studying the issue further. Japan is creating a study commission but shows no inclination to move rapidly.

Both the Council of Europe (a strictly European, human rights-oriented organization) and the OECD (whose membership includes most advanced Western European countries, the U.S., Canada, Japan, and Australia) have been actively studying the issues. The Council of Europe has drafted a privacy protection convention, while OECD is both studying the economic and social aspects of international information flows, and is engaged in drafting guidelines for harmonizing disparate national privacy legislation.

The European approach to privacy protection is generally to enact broad, omnibus legislation which covers all types of automated government and private sector records and which is implemented and enforced by a governmental bureaucracy. The Europeans stress that their intent is not only to establish standards for protection of personal information, but also to make important social statements about the relationship of the citizen to the state.

Parenthetically, the U.S. is by far the most important partner in international information exchanges and in the information processing industry, dominating world markets

in computer software, hardware, and data processing. This dominance is well understood in other advanced countries, and to some uncertain degree may lie behind the sudden surge of concern for privacy protection. That is, the impetus for foreign privacy protection laws may lie not only in a genuine concern for the civil rights of local citizens, but also in an effort to blunt U.S. dominance of international information processing. The latter arises out of feelings of nationalism, concern for sovereignty, and economic control.

At the same time, Europeans are also concerned about the export of personal information to the U.S. in the absence of adequate privacy protection in the U.S., and some European legislation can be interpreted to bar such export. Finally, Europeans are particularly concerned about the lack of a central governmental office to assist foreign nationals in the protection of their privacy rights within the U.S.

In the international arena, the U.S. has several interests at stake: protecting the privacy of U.S. citizens concerning records maintained abroad, preventing the development of non-tariff barriers under the guise of privacy protections, and encouraging the free international flow of information. While the European activity to date presents no immediate threat to U.S. interests, the development of a comprehensive domestic privacy policy will greatly strengthen our ability to safeguard U.S. interests in the future.

G. The Elements of a Privacy Policy

The remainder of this Part presents an overview of the basic elements of a general privacy policy as that policy might be applied to the non-Federal sector. It concludes with a proposed implementation strategy.

In Part II, each of the nine industries and record-keeping relationships examined by the Commission is described and the decisions for application of this general policy to those industries and record-keeping relationships are discussed.

1. Notification of Information Collection Practices

Objective

During the course of the business relationship between an organization and an individual, the organization may collect personal information about the individual from many sources. The first objective of a privacy policy is to give the individual some influence over an organization's information collection practices by requiring it to provide prior notice of the kinds of information it may seek and the types of sources that may be contacted, and to limit its information collection practices to those stated in a notice. This alerts an individual to the personal information that will be compiled about him as a result of entering into a record-keeping relationship.

Current Law and Practice

At present, individuals are given little or no information about an organization's information collection practices. Thus, individuals are unable to make informed choices between competing organizations on the basis of their collection practices. Nor are individuals able to judge whether the good or service sought from an organization is worth the potential invasion of their privacy.

Federal and state legislation in this area is limited. It imposes requirements on only a few record keepers, and those laws generally do not require a notice whenever information is collected about an individual. The Fair Credit Reporting Act, for example, requires only that institutions such as credit grantors, employers, and insurers notify an individual if they request an outside agency to prepare an investigative consumer report (a report prepared through personal interviews

with friends, neighbors, and other acquaintances concerning the consumer's character, general reputation, and mode of living). If the consumer makes a written request, he must be provided with a notice describing the "nature and scope" of the investigation. However, this requirement, applies only if the report is obtained from a consumer reporting agency; it does not apply if the user of the report performs the investigation itself.

Discussion

The Privacy Commission proposed that an organization be required to give the individual notice at the start of the business relationship of the kinds of information it may seek from third parties and the types of sources that may be contacted in the course of evaluating the application and maintaining the relationship. With this information, the individual can know what to expect before entering into a business relationship with the organization. In turn, the organization is limited to the information collection practices stated in the notice, unless it subsequently obtains the individual's consent to conduct an investigation or collect information not stated in the notice. Past experience with laws requiring a notice of collection practices such as this, including the Privacy Act of 1974 and the Fair Credit Reporting Act, suggests that just the fact of notification will help eliminate unnecessarily intrusive or otherwise objectionable collection practices.

The requirement for notification of and limitations on collection practices is, however, no cure-all. First, it establishes only a procedural requirement that information collection practices be limited to those stated in a prior notice; it does not limit what that notice may contain. Moreover, in most industries, a model notice probably will be developed and adopted by the major companies, thereby limiting the competition among companies on the basis of collection practices. Second, because of extensive notices already required by other laws, there is a danger of information overload. One possible approach is to adopt a two-step process whereby the individual is automatically given only the most general notification, but is advised of his right to request and receive a more detailed notice.

2. Propriety and Relevance of Information Collected

Objective

Another basic privacy objective is to limit the collection and use of information which may be improper or irrelevant to the decision-making process which gave rise to its collection. For example, a person's race and sex may be statistically relevant to a credit decision, but society has decided in the Equal Credit Opportunity Act that it is improper to base credit decisions on such criteria. An allied concern involves the collection of proper and relevant information through means which society may consider improper, e.g., through pretext interviews in which the source is misled into supplying information, or through the use of truth verification devices (i.e., "lie detectors"). The Commission proposed that governmental mechanisms should exist to consider individual citizen complaints about propriety and relevance on a problem-by-problem basis. It made specific proposals to prohibit the use of pretext interviews and truth verification device in certain contexts.

Current Law and Practice

There are few prohibitions on the private sector's collection of information. Most relevant laws prohibit only the use, but not the collection, of specific types of information. The Equal Credit Opportunity Act, for example, prohibits the use of sex, marital status, race, religion, and certain other characteristics as the basis for a credit decision. However, it permits collection of some of this information, e.g., marital status, which may affect the creditor's collection rights. It also requires collection of other information, e.g., race, to monitor discriminatory mortgage lending practices.

The Fair Credit Reporting Act's original draft contained general relevancy requirements, but they were removed in the face of heavy industry opposition. The Act does impose, with some significant exceptions, a prohibition on reporting adverse information more than seven years old (which is a form of relevancy requirement).

The only existing model of a general standard of propriety and relevance is the Privacy Act, which requires Federal agencies to maintain, use, and disseminate only records which are relevant and necessary to accomplish a lawful agency purpose. The Act also prohibits collection of information concerning an individual's exercise

of his First Amendment rights, except when collected for law enforcement purposes. According to the Commission, however, these requirements have had little impact on Federal record-keeping practices.

Laws proscribing the use of what may be excessively intrusive collection techniques by private sector organizations are similarly limited. The use of truth verification devices is regulated at the state level on an irregular basis, and only a few states now prohibit their use. Truth verification devices are barred from use in Federal employment by Civil Service Commission regulations. The Federal Trade Commission has found pretext interviews to be unfair or deceptive for businesses under its jurisdiction, and the recently enacted Fair Debt Collection Practices Act prohibits the use of these practices by debt collectors.

Discussion

The Commission proposed that there be formal governmental mechanisms to consider citizen complaints and raise questions of relevance and propriety on a case-by-case basis. This proposal was based upon the belief that certain information simply should not figure in business decisions--that it is of no concern to anyone but the individual himself. The Commission specifically rejected two alternative approaches to this issue: (1) to create general statutory requirements on the relevance and propriety of information for subsequent definition by a regulatory agency or the courts; and (2) absolute prohibitions on the collection and use of certain information (e.g. sexual preference, political affiliation, etc.) by all record-keeping organizations.

Industry opponents of any propriety and relevance requirements raise First Amendment objections to prohibitions on the free flow of information. Industry argues that market forces already influence businesses not to collect irrelevant information. Industry fears that any relevancy requirements will lead to limitations on the right to obtain information needed to make business decisions. With these concerns in mind, as well as the difficulty of determining what information is irrelevant to any possibly legitimate business use, the Commission for the most part refrained from specific prohibitions and opted for future case-by-case consideration.

Two specific questions concerning the propriety and relevance of information collected will be raised for decision:

1) Should the use of lie detectors be prohibited in employment decisions (considered in Part V).

2) Should a mechanism exist for challenging the relevance and propriety of information collected and used by credit grantors and insurance companies. (Part II.)

3. Individual Access to Records

Objective

The third privacy objective is to entitle an individual to see and obtain a copy of any reasonably retrieveable personal information concerning him which is held by a non-Federal record keeper.

Current Law and Practice

At present, the Privacy Act allows an individual access to records maintained about him by the Federal government. However, no such general right of access exists in the private sector. The Fair Credit Reporting Act (FCRA) gives an individual the limited right to learn the "nature and substance" of records held by a consumer reporting agency, but this does not mean that the individual can see the actual information in the records. The FCRA also does not apply to the records of credit grantors, depositories, insurers, and employers who may use these reports to made decisions about individuals. In the credit area, as a rough substitute for actual access to records when a billing dispute occurs, the Fair Credit Billing Act requires a credit-card issuer to provide a consumer with a written explanation of any disputed billings and copies of documentary evidence of indebtedness.

In practice, many record keepers in the non-Federal sector do allow individuals to see and obtain copies of their records. Banks and credit-card issuers generally send the individual a monthly account statement which reflects a summary of the billing records which they maintain; many employers now permit employees access as a matter of good personnel practices. Partially in response to repeated criticism, the major consumer reporting agencies now allow an individual to see and copy a consumer report about him. However, the procedures developed for access are sometimes difficult for an individual to use and these are not rights provided in law.

Discussion

Individual access to records is a precondition to several of the other basic elements of a privacy policy. For example, a right of access enables the individual to determine whether the records contain information beyond the scope of the prior collection notice (if such notice is required) and to challenge the accuracy of the information

contained in the records. Merely extending the right to learn the "nature and substance" of what is in the record has proven in practice with the Fair Credit Reporting Act to be insufficient. "Nature and substance" is determined by the record keeper, and in the past record keepers have failed to adequately inform the individual of the records' contents, either intentionally or out of lack of knowledge about what the individual considered important.

Assuming that only reasonably retrieveable records need be disclosed and that the organization's copying costs may be recovered, there is little problem in the effected industries with allowing individuals to see and copy their records. However, the situations in which such access occurs and, with some record keepers, the records to which access is allowed are questioned.

4. Correction and Amendment of Records

Objective

The fourth privacy objective is to provide an individual with the ability to challenge the accuracy of information about him maintained by non-Federal record keepers. If the individual believed the information were inaccurate, he would be entitled to bring the supposed inaccuracy to the record keeper's attention. The record keeper then would be obliged either to make the correction or to reinvestigate the disputed matter. If, after reinvestigation, the record keeper determined that the disputed information is accurate, the record keeper would have to indicate that the matter is in dispute and include the individual's version of the dispute in the record. The amended record would then have to be sent to prior and future recipients of the record, and, in some instances, to the source of the disputed information. Similarly, if a record keeper itself discovers a significant inaccuracy which it corrects in its own record, then it should also take reasonable steps to propagate that correction.

Current Law and Practice

At present, there are no uniform requirements that non-Federal record keepers allow an individual to correct and amend records about him. The Fair Credit Reporting Act (FCRA) provides consumers with a right similar to that outlined above to dispute the accuracy of consumer reports. With regard to Federal government records, the Privacy Act provides a general right to challenge the accuracy of recorded information similar to that provided by the FCRA. The Fair Credit Billing Act sets forth a specific procedure for resolving billing disputes, and requires reinvestigation by the record keeper. Under common law, a business which reports erroneous information could be sued for defamation or libel, but the individual would usually be required to prove that the information was furnished with malice or willful intent to injure.

Discussion

Some record keepers contend that market forces provide a significant incentive to correct clearly inaccurate information brought to a record keeper's attention by an individual. First, a change in the information may permit the record keeper to do business otherwise

foregone. Second, the record keeper has a general interest in good customer relations. However, if the inaccuracy is not obvious or is the result of an underlying error in the organization's records, there is generally little incentive for the organization to reinvestigate the matter. Nor is there a great incentive to send corrections of the record to other record keepers. Also, not many record keepers permit an individual to file a statement of his version of the facts.

Finally, requiring an organization only to propagate corrections made by the individual ignores the possibility that the organization itself may discover and correct an error which, if left uncorrected in the files of other record keepers, could cause equal harm to the individual. Entitling an individual to challenge the accuracy of information is an important device for promoting the accuracy, timeliness, and completeness, of information maintained by the record keeper, but, from the individual's point of view, it is a partial safeguard if the record keeper is not obliged to send corrections to other record keepers.

## 5. Reasons for Adverse Decisions

### Objective

The fifth privacy objective deals with an individual's rights after a private sector organization decides not to provide a benefit or service, or decides to offer it on terms less favorable than usual. The objective is to allow an individual to know the specific reasons for the decision and the specific items of information which are alleged to support the decision.

### Current Law and Practice

The Equal Credit Opportunity Act (ECOA) requires disclosure of the specific reasons for an adverse credit decision. Credit grantors typically provide this information by a form checklist. The disclosure may be made either automatically or upon the request of the individual. The Fair Credit Reporting Act (FCRA) requires that an individual be notified when information from a consumer reporting agency is used in making an adverse credit, insurance, or employment decision. Unlike credit grantors (which are covered by the ECOA), insurers and employers are not required by statute to inform the individual of the reasons for an adverse decision. Some state insurance statutes entitle an individual to know why a policy was denied or cancelled, and at least one state (Virginia) has passed a statute providing consumers with the right to know the specific reasons for an adverse action on an application for insurance.

### Discussion

A right to learn the reasons for the denial or termination of credit, insurance, or other benefits is the beginning step in consumer due process. The adverse decision may have been made on the basis of incorrect information or for reasons which are illegal, irrational, or against public policy. Although a right to learn the specific reasons for an adverse action, as well as any supporting information, would not allow the individual to require the institution to reconsider its decision to deny a benefit or service, it would enable the individual to provide supplemental information that the institution could use if it wished to reconsider its denial. Also, in addition to allowing the individual to have an adverse decision reversed in many cases, this right would enable the individual to challenge any decision criteria or information collection practice he thought improper or illegal.

Experience with the ECOA demonstrates the usefulness of this right. The Federal Reserve Board recently studied the effects on nine large creditors of the ECOA's requirement that creditors inform rejected credit applicants of the reasons for the denial, either automatically or on request. The Federal Reserve Board discovered that a substantial portion (12-23%) of the rejected applicants requested the reasons for the denial when those reasons were not given automatically. From 30-70% of those who requested the reasons then supplied more information; and from 25-72% of those supplying more information were then granted credit. Comparable results occurred when consumers were automatically provided the reasons for adverse decisions.

Significant portions of private industry can be expected to oppose the requirement that an individual be informed of the reasons for an adverse decision. Even those supporting it fear that it might be implemented in such a way as to prove costly and otherwise burdensome.

6. Accuracy, Timeliness, and Completeness of Records

Objective

An important consequence of viewing privacy as a matter of fairness is the stress placed upon the objective of the accuracy, timeliness, and completeness of the information used in making a business decision and disclosed by a record keeper to another decision maker. Of course, the expectation is not that records will ever be entirely error free. Rather, the aim is to assure that accuracy, timeliness, and completeness of records will be maximized.

Current Law and Practice

In the Federal sector, the Privacy Act requires that an agency "maintain all records which are used by the agency in making any determination about any individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination."

The Fair Credit Reporting Act requires consumer reporting agencies to adopt "reasonable procedures" to ensure the accuracy of the information they obtain and report. The nation's largest investigative reporting agency was recently found in violation of this standard by an FTC administrative law judge. The decision in this case, in which the company has been ordered to significantly alter its operating procedures and record-keeping practices, is being appealed.

Apart from these provisions, record keepers are under no general legal obligation to cause reasonable steps to be taken to assure the accuracy, timeliness, and completeness of recorded information.

Discussion

The Privacy Commission identified two basic approaches to ensuring the accuracy, timeliness, and completeness of information collected, maintained, and disclosed by private sector record keepers. First, a law could establish a general standard of record-keeping performance and require organizations to take "reasonable procedures" to satisfy that standard. To enforce compliance, government agencies and individuals could be given a right of action against institutions whose record-keeping

practices did not satisfy this standard. In addition, government agencies could, if appropriate, be authorized to issue implementing regulations to define practices and procedures necessary to comply with the general standard.

A second approach would be to create in law specific procedural rights and requirements addressing the problems identified in an industry or record-keeping community. In this approach, the objective of ensuring the accuracy, timeliness, and completeness of records would be sought by granting the individual the other rights discussed in this section (i.e., to see, copy, correct, and amend his records), and by requiring the record keeper to propagate corrections, rather than by holding the organization to a general standard. This approach, too, would be enforced by giving individuals and government agencies a right of action against the record keeper. However, the government enforcement role here would be more limited, since there would be no need for regulations to define the practices which comply with the specific statutory requirements.

In general, the Privacy Commission favored the second approach, and opposed placing a general record keeping standard on private sector record keepers. In the public sector, however, the Commission generally favored placing a general standard on the record keeper. The Commission believed that there is a substantial difference between applying a general "reasonable procedures" standard to the government and to private sector record keepers. The primary concern is that such a general standard applied to private sector record keepers would necessarily entail extensive government involvement in the record-keeping practices of private businesses. However, this concern obviously does not apply in the context of governmental entities, which are by definition subject to such scrutiny. Even those in private industry who support some sort of privacy protection legislation generally agree with the Commission's position of no general standard for accuracy, timeliness, and completeness.

The Commission believed that creating specific rights and procedures would allow the individual more effective control over the accuracy, timeliness, and completeness of his records, and that adoption of a general standard would lead to high compliance costs, arising primarily from protracted litigation to determine what record-keeping practices would satisfy the standard. Finally, the Commission argued that its approach would place

the economic burden of compliance mainly on those organizations with poor record-keeping practices and which fail to treat their customers in a responsible manner.

The staff of the Federal Trade Commission, on the other hand, favors a general record-keeping standard for accuracy, timeliness, and completeness in the belief that such a standard is a necessary component of any comprehensive privacy policy. They believe that allowing an individual rights of access and correction should not be the only means by which the quality of records is maintained, and that the record keeper should bear an affirmative responsiblility to monitor its own record-keeping practices to prevent errors from occurring originally.

They counter the argument that a general requirement will be burdensome and costly by suggesting that it would impose the general incentive to ensure that accuracy is given sufficient consideration in making information handling and system design decisions, without encumbering systems with specific, and perhaps inflexible, rules. Moreover, they point out that government regulation under such a standard, if drawn at all, need do no more than specify minimum requirements for such activities.

These two approaches are not mutually exclusive, although they do represent different philosophies of government regulation. Both could be in place at the same time. The industry-by-industry decision section which follows (Part II) will consider application of both the specific procedural rights and requirements dictated by the Privacy Commission approach, and, where potentially appropriate, a general record-keeping standard for accuracy, timeliness, and completeness.

## 7. Confidentiality and Disclosure of Information

### Objective

The final objective of a privacy policy is to protect the confidentiality of personal information held by credit institutions, banks, insurance institutions, and medical care providers, and of telephone toll records. Much of this information is highly personal, e.g., financial and medical information, and therefore arguably should be held in confidence.

### Current Law and Practice

The Supreme Court has held that the individual has no legally enforceable expectation of confidentiality under the Fourth Amendment for financial records maintained by banks. (United States v. Miller, 425 U.S. 435 (1976)). A similar lack of legal protection exists for insurers, medical-care providers, and providers of telephone services. This means that, when the government asks a private sector record keeper to disclose personal information about an individual, the individual has no legal right to be notified of, or contest, the government's acquisition of those records. Nor does the individual ordinarily have a right to be notified of or to control the record keeper's voluntary disclosures of information to the government or others. In short, the individual has no legally enforceable expectation of confidentiality for the personal information which a private sector record keeper holds about him.

### Discussion

The balance of this section develops one aspect of what the Privacy Commission labeled "an expectation of confidentiality": namely, the record keeper's obligation to maintain the confidentiality of certain records. Questions of government access to private sector records are discussed in Part III.

The Commission proposed, and the responding agencies generally thought it desirable, that, for credit grantors, depositories, insurers, medical-care providers, and telephone toll records, a legally enforceable expectation of confidentiality should be created and disclosures to others within the private sector should be constrained.

This proposal contains both procedural and substantive controls on disclosures. Procedurally, at the beginning of his relationship with an organization, an individual would be given a notice describing the disclosures which may be made of information obtained in the course of that relationship. A record keeper could then disclose information only if the disclosure is:

1) consistent with the terms of the notice;

2) required or authorized by law (including the various forms of legal process which will be discussed in Part III); or

3) specifically authorized by the individual to whom the record pertains.

If the record keeper fails to fulfill this obligation and improperly discloses personal information, the individual would have a legal right of action and could receive damages of up to $10,000 from the record keeper.

As a substantive control, the notice given by the record keeper must include a "reasonably specific" description of all the allowable disclosures the record keeper intends to make. Other than (2) and (3) above, the only allowable disclosures are those which are:

1) necessary to service the relationship (e.g., from a credit grantor to a credit bureau);

2) necessary to protect the record keeper against the individual (e.g., in the event there is reason to suspect fraud); or

3) necessary to protect the individual (e.g., in the event of a medical emergency).

If a disclosure is not within one of these allowable categories, it cannot be included in the notice and thereby made automatically by the record keeper. The requirement that the notice's description of disclosures be "reasonably specific" is, of course, a critical factor whose actual meaning, like all statutorily imposed "reasonableness" tests, will have to evolve. If the description is too vague, there will be no effective control. If the description is too specific, the requirement will prove burdensome to implement. Of course, there may still be instances in which an organization wishes to change its record-keeping practices so dramatically

that it is necessary to seek the consent of its customers for the new disclosure pattern.

This proposal would allow the individual to participate in the process of disclosure and would give him some control, or at least influence, over the confidentiality with which his records are kept. While this may be important to a person's feelings of privacy, its actual constraint on private sector record keepers' disclosure practices will depend in part upon what disclosures are determined to be necessary to "service the relationship." However, establishing a legal duty on the record keeper and giving the individual a right of action to enforce the obligation represents a significant shift in the current legal structure governing the confidentiality of records.

8. Implementation

The Privacy Commission, in suggesting an implementation strategy for its recommendations, attempted to minimize government regulation and to bring about adequate enforcement of its recommendations with a minimum of cost to both the individual and the record keeper. Most of the Commission's recommendations do, however, specify mandatory measures. In part, the Commission chose a statutory approach because it believed that voluntary compliance would be too uneven to be dependable; but more importantly, many of the issues are legal ones and require legal remedies. In the Miller case described above, for example, if the bank had wholeheartedly tried to protect Miller's interest, it would have done him little or no good since, under existing law, Miller would have no legal interest in the records to assert.

The primary mode of enforcement adopted by the Commission was to provide an individual a right to sue to force an institution to comply with one or several of the objectives. For example, an individual could sue in court to obtain a copy of a record about him or to require the correction of a particular item of information if a record keeper failed to do so. In addition to being able to enforce compliance with the specific requirements, an individual who was successful in court would be given attorney's fees and damages of up to $1,000. This provision was intended to encourage individuals to exercise their rights.

In general, the Commission did not propose that an individual be able to obtain general damages for most violations of his rights. However, the Commission did recommend that, where the institution has violated an individual's expectation of confidentiality, the individual would be able to recover actual damages and, if the institution acted willfully or intentionally in violating an individual's expectation of confidentiality, the individual could be awarded general damages in the amount of at least $1,000, but not more than $10,000. The Commission believed that the greatest possible harm to the individual occurs when information is disseminated outside of the institution, and so recommended that an individual be able to recover damages for such a loss.

As a second aspect of its implementation strategy, the Commission recommended that Federal agencies with existing enforcement authority be able to force institutions

to comply where there have been repeated violations, because individuals are not always in a position to assert their own rights. The Commission also recommended that existing agencies with expertise in particular fields should enforce the recommendations in each of their own areas of responsibility. In doing so, the Commission explicitly rejected the concept of a centralized privacy enforcement function in relation to the private sector.

The Commission believed that this implementation approach would substantially burden only those institutions who refuse to follow the objectives in good faith. There would be no general compliance costs, such as annual filings or registrations. Only those institutions which are brought into court by individuals or the government for failing to comply would have to bear the costs of justifying their practices and procedures.

Finally, the Commission followed the approach of the Fair Credit Reporting Act in establishing minimum Federal standards, but not restricting the states in going further than the Federal statute. For example, under the FCRA, Federal law requires a credit bureau to inform an individual of the "nature and substance" of information it possesses about him. Various states (including California and Maryland) go one step further and require the credit bureau to give the individual an actual copy of his report. The Commission adopted this approach in response to the great concern of private sector institutions over the danger of duplicative or conflicting requirements in both the Federal and state levels, and believed that it was appropriate throughout the private sector.

Area of Agreement

Except as otherwise indicated in the remainder of this memorandum, the basic implementation strategy proposed by the Commission has been assumed for the purposes of drafting this memorandum. While the agencies have not spoken directly to the issue of implementation strategy, except as indicated below, their responses to the specific recommendations of the Commission suggest agreement with the Commission's implementation strategy.

## II. Non-Federal Records

### A. Introduction

This part presents for decision the issues involved in applying the basic privacy package discussed in the previous section to non-Federal record keepers. This includes the major record-keeping industries in the private sector (credit, depository, and insurance), as well as the other record-based "relationships" which individuals maintain with organizations (employment, medical care, education, and public assistance and social services). These are the record relationships that were studied by the Privacy Commission, and to which the bulk of the Commission's 162 specific recommendations were directed.

Each industry or record-keeping relationship is considered separately. First, the industry and its characteristic record-keeping problems are discussed, including an examination of current law and practice. Next, in summary form, those areas of agreement among the Privacy Commission, the agencies, and the affected industries and groups are presented. Since the indicated areas of agreement parallel the elements of a basic privacy policy presented in the immediately preceeding section, there is no specific discussion of the "pros" and "cons." Finally, the issues which require decision are presented. Generally, these are questions which raised significant disagreement between the Commission, the agencies, and the affected private sector record keepers.

Unless otherwise indicated, a single, general term is used to encompass the full range of institutions within an industry or record-keeping community. For example, the term "insurance institutions" is used to refer not only to insurers, but also to the information support organizations within the insurance industry, such as indexers of information, like the Medical Information Bureau (MIB), and consumer reporting agencies.

Finally, any characterization of the position of industry with respect to a particular proposal is inevitably a condensation of varying, and sometimes conflicting, points of view. In particular, an indication of industry support for a particular position does not necessarily mean that industry would affirmatively seek passage of legislation incorporating that position; rather, in some cases, it indicates only that industry accepts the position, either for substantive or political reasons.

B. Consumer Credit Industry

Description of the Record Relationship

It is the rare American household that does not have some sort of consumer-credit relationship. Banks, savings and loan associations, finance companies, credit unions, and retailers are the principal providers of this service. As the amount of consumer credit has increased in our society, so has the reliance of these institutions upon recorded information about individuals in establishing and maintaining credit relationships. This, in turn, has led the credit industry to vastly expand its facilities for sharing information on individuals, especially through credit bureaus, the traditional vehicle for such interchange.

Typically, local and national credit bureaus collect and maintain information on an individual's previous and existing lines of credit, payment history, financial status (income and employment), and public-record information, such as bankruptcies. They collect this information from credit grantors, many of whom, such as the large retailers, provide the credit bureaus with periodic updated reports on each of their credit customers. The credit bureaus distribute this information to other credit grantors for use in evaluating an applicant's credit worthiness and to other credit bureaus, collection agencies, inspection bureaus, insurers, and employers who use it for a variety of purposes.

Credit card issuers rely heavily upon recorded information not only in establishing a line of credit, but also in documenting its use. They continually collect and maintain information to enable their card holders to identify the various transactions made--e.g., name of merchant and goods or services provided.

The popularity of credit cards has led to a dependence on an elaborate authorization system to control customer fraud and overextension. Credit-card authorization services keep records showing which cards are cancelled, overextended, or stolen. Merchants check with these authorization services before accepting cards. To maintain the information base, card issuers routinely disclose their negative information to the service, which reports to subscribers, such as airlines, hotels, and restaurants.

Check authorization and guarantee services serve a similar function regarding individuals who have written bad checks. Check authorization services determine

for their subscribers whether an individual has a recent history of writing bad checks; check guarantee services guarantee payment.

Automation has greatly increased the speed and efficiency with which information is collected and exchanged within the credit industry. In addition, it has changed the manner in which credit decisions are made. Credit decisions are now frequently made through a technique called "point-scoring," by which a credit grantor statistically rates an applicant's key personal characteristics and produces an overall rating of credit worthiness. While this system has its economic advantages, it diminishes the individual's opportunity to challenge the basis of a credit decision, since he has greater difficulty in isolating the factors which caused a negative decision.

Current Law

The information practices of the credit industry are already regulated by the Fair Credit Reporting Act (FCRA), the Equal Credit Opportunity Act (ECOA), and the Fair Credit Billing Act. The ECOA proscribes the use of race, sex, marital status, and some other kinds of information in credit decisions, and requires that the reasons for an adverse decision be disclosed if the individual so requests. When an individual asks for these reasons, creditors usually respond with a form checklist. Credit grantors are currently not required to disclose the specific item(s) of information supporting those reasons, as the Privacy Commission recommendations discussed below would provide. Credit grantors are, however, required by the FCRA to notify the individual whenever information supplied by a credit bureau is used in making the adverse decision, and to give him the name and address of the credit bureau. A credit grantor is not required to disclose to an individual the contents of a credit report that served as a basis for an adverse decision; in fact, a credit bureau's contract with the credit grantor usually precludes this. If the consumer wishes to learn the contents of the credit bureau's report, he must go directly to the credit bureau.

The information practices of credit bureaus are the most regulated of all private sector record keepers. The Fair Credit Reporting Act gives the individual the right to know the "nature and substance" of his credit bureau record and to file an explanatory notice when he disputes its accuracy. The FCRA also requires credit bureaus to adopt "reasonable procedures" to

assure the accuracy of the information they report to subscribers.

Areas of Agreement

There is agreement among the Commission and most agencies responding that, in the area of consumer credit, Federal law should require:

a) that credit grantors notify individuals at the time of application for credit of their collection and disclosure practices, and follow that notice;

b) that individuals have the right to automatically be given the reasons for an adverse credit decision; and, upon request, to see and copy the specific item(s) of information used in making that decision;

c) that credit grantors promptly send any corrections of inaccurate, untimely, or incomplete information to credit bureaus, debt collection agencies, or authorization services to whom the inaccurate information has previously been disclosed;

d) that credit authorization services be covered by the requirements placed upon credit grantors and credit bureaus (including the requirements placed on consumer reporting agencies by the Fair Credit Reporting Act), except for the requirement to propagate corrections (in (c) above);

e) a legally enforceable expectation of confidentiality (as defined in Section I.G.7); and

f) enforcement by:

(i) an individual right of action, and

(ii) the FTC or bank regulatory agencies for repeated or systematic violations.

Areas of Disagreement

1. Should an individual have a right to see and copy at any time all reasonably retrieveable records about him held by a credit grantor, not just the items of information that have been used to make an adverse decision (as set forth in 1(b) above).

Pro:

To provide for access to consumer credit records only after an adverse decision is inconsistent with the approach the Commission took in other areas. Arguably, an individual should be able to avoid an adverse decision by correcting erroneous information before the decision is made. In addition, if an individual is denied credit based on information reported by a credit grantor other than the one to which he is applying, he will need access to the reporting creditor's records. While the Fair Credit Billing Act provides some help in this situation, it does not apply to all creditors (e.g., closed-end credit relationships are excluded) and must be used within 60 days of when the error occurs. A general right of access to all credit information will allow the individual to correct such information. The Department of Commerce and the National Credit Union Administration suggested this provision.

Con:

The Privacy Commission recommended that an individual have access to his credit records only when an adverse decision has been made about him and only to those records that a credit grantor has used to make that decision. This differs from other areas, such as insurance, where the Commission recommended a right of access to all information at all times. The Commission made this distinction because an individual usually receives a monthly statement of his credit account, which in combination with the records that might be used to make an adverse decision, comprises all the records that a credit grantor commonly maintains on the individual. The Commission believed that it would unnecessarily burden credit grantors to require them to assemble and disclose at any time the information they regularly make available as part of a monthly billing cycle. The credit industry would prefer no right of see and copy, but if such a right were granted, would prefer that it be provided only in the instance of an adverse decision and include only the records used in the decision, thereby reducing retrieval costs. The Department of the Treasury supports the Privacy Commission recommendation.

Decision:

_____ Yes, the individual should have a right of access to all credit records upon request.

_____ No, an individual right of access to credit records should be limited to those records that have been used to make an adverse decision about him.

2. Should an individual have access to credit records about him maintained but not prepared by the institution from which he seeks the records, e.g. credit reports in the hands of a credit grantor?

Pro:

The Commission recommended that an individual have direct access to all records maintained by a credit grantor, and the responding agencies, while endorsing the general recommendation, did not speak directly to this specific issue. This is intended to close a current gap in consumer credit law. The Equal Credit Opportunity Act requires a credit grantor to disclose the reasons for an adverse decision, and the Fair Credit Reporting Act requires that the consumer be told if the decision was based "in whole or in part" on information obtained from a consumer reporting agency. However, by contract the credit grantor cannot disclose the report which was used. The consumer must now go directly to the credit bureau to get his file, yet the credit bureau does not know why the adverse decision was made. The Commission's recommendations would allow the individual to be informed of the reasons for an adverse decision and see the information used in that decision in the same place.

In addition, it is possible that the credit bureau may not know what information it gave to the credit grantor. Because credit bureaus regularly update their files, the information that the individual eventually gets from a credit bureau may not be the information that the credit grantor received and used to make an adverse decision.

Con:

The credit industry, particularly the credit bureau

industry, opposes this requirement. Credit bureau reports are coded and must be interpreted to the consumer. Although it is feasible for the credit grantor to interpret the report for the consumer (they already interpret it for their own use), credit bureaus would prefer to do so themselves, particularly since they may ultimately be liable if the consumer sues for negligent or willful defamation. Also, credit bureaus already have employees trained to interpret the reports for consumers, and credit grantors would prefer not to train their own employees for this purpose.

Decision:

_____ Yes, an individual should have a right of access to credit records about him maintained but not generated by the institution from which he seeks the records.

_____ No, an individual's right of access to credit records should be limited to those records generated by the institution from which he seeks the records.

3. Should there be a mechanism for the individual to challenge the relevance and propriety of information collected or used by credit grantors?

The Commission did not recommend that a single Federal agency be assigned this responsibility, but suggested that appropriate authority be vested in the Federal Home Loan Bank Board, the Federal Reserve Board, and other regulatory agencies responsible for enforcing the Fair Credit Reporting Act. The Commission was specific, however, in recommending that the mechanism not involve direct regulatory control by a Federal agency on questions of relevance and propriety. As envisioned by the Commission, the mechanism would collect consumer complaints about the information practices of the industries they regulate and report to Congress as to the need for legislation to control the collection or use of any particular items of information. An example might be that the Federal Reserve Board would suggest legislation prohibiting the collection of information indicating sexual preference for use in credit decisions.

Pro:

The Commission, the Department of Commerce, and the National Credit Union Administration support this proposal. Individuals may be frustrated by what they believe to be overbroad and irrelevant or improper requests for information. Often they do not have the market power to prevent its collection. A government agency, such as the Federal Reserve Board or the Federal Trade Commission, could consider consumer complaints and suggest remedial legislation as needed on a case-by-case basis.

Con:

The credit granting and credit reporting industries uniformly and vehemently oppose this recommendation, which is also opposed by the Federal Reserve. Industry believes that the marketplace discourages the collection of irrelevant or improper information and that there is a trend to collect less information. Industry argues that most information is relevant to some business purpose, and does not want government interference in business decisions about what information to collect.

To the extent problems once existed, industry also believes that they have been resolved by the Equal Credit Opportunity Act, which prohibits the use of marital status, sex, age, religion, national origin, or race in making credit decisions.

Decision:

_____ Yes, there should be governmental mechanisms for the individual to challenge the relevance and propriety of information collected or used by credit grantors.

_____ No, such mechanisms should not be created.

4. Should Federal law require that a credit grantor have reasonable procedures to ensure the accuracy, timeliness, and completeness of the personal information it collects, maintains and discloses?

For a general discussion of this issue, see Section I.G.6, "Accuracy, Timeliness and Completeness."

Option 1: All credit grantors:

It is the position of the FTC staff that a "reasonable procedures" standard for accuracy, timeliness, and completeness similar to that contained in the Fair Credit Reporting Act (15 U.S.C. 1681e(b)) for credit bureaus is a necessary component of a comprehensive privacy policy applied to credit institutions. Current law is unbalanced in its coverage of the information practices of the credit industry. The industry depends heavily upon the exchange of information, with credit bureaus serving as the information brokers, or go-betweens, for the industry. In addition to using credit bureau reports for evaluating consumer applications for credit, credit grantors regularly report to the credit bureaus on the state of their consumer accounts; thus, they are both providers and receivers of information as it flows within the industry. While credit bureaus are required to have reasonable procedures to assure the accuracy of the information they report, credit grantors are under no such requirement regarding the information they report to one another, either directly or through the intermediary of a credit bureau. The imposition of such a requirement would erase the often artificial distinction currently drawn between credit bureaus and their sources of information (credit grantors).

The FTC staff, which has primary enforcement responsibility for the FCRA, has found that placing the "reasonable procedures" requirement on credit bureaus has, among other effects, caused them to maintain routine procedures for correction of gross errors in the information they process and disclose. However, the impact of these procedures has been limited by the absence of a legal requirement on the credit grantor to ensure the overall accuracy of the information it supplies to the credit bureau, and the fact that the credit bureau is not in a market position to influence the credit grantor to report only accurate information.

The FTC staff has also identified specific problems related to the absence of standard codes for information reported by credit grantors, the filing of adverse credit reports by credit grantors even after signing a general release for partial payment of a disputed debt, and in the identifying information used in credit grantor reports to credit bureaus.

The FTC staff believes that a requirement that a credit grantor adopt "reasonable procedures" to ensure the accuracy, timeliness, and completeness of records would help solve some of these problems.

Finally, while the FTC staff would endorse the Commission's proposal concerning the accuracy of information reported by credit-card issuers to credit authorization service (see Option 2, below), it would argue that the proposal addresses only a small portion of the identifiable problems in the credit industry. The FTC staff believes that a general requirement is preferable to the more specific and limited remedies recommended by the Commission. Note that this option was not considered by the agencies in the review process.

Option 2: Only credit-card issuers' reports to independent authorization services:

In contrast to Option 1, which addresses all reports made by all consumer credit,grantors, this recommendation addresses only one class of credit grantors (credit-card issuers), and then only the reports they make to independent authorization services. It does not cover reports made by credit grantors to credit bureaus and other credit grantors.

The Commission recommended that Federal law require a credit-card issuer to have reasonable procedures to assure that the information it disclosed to an independent authorization service is accurate at the time of disclosure. However, it explicitly rejected recommending that a Federal statute require all credit grantors to adopt reasonable procedures to ensure the accuracy, timeliness, and completeness of their records as a separate, general rule. The Privacy Commission position is supported by the Commerce Department, the National Credit Union Administration, and the Federal Reserve Board.

The Privacy Commission made its specific recommendation concerning authorization services because they act preemptively. An individual thus has no way of rectifying an error in an independent authorization service record in time to affect that transaction when his use of his credit card to pay for goods or services is refused because of negative and incorrect information from an authorization service. Procedures to correct inaccuracies after the fact, therefore, do little good in this instance.

The Privacy Commission's rejection of a general "reasonable procedures" standard was based on the belief that the identifiable problems in consumer credit will be adequately remedied by the combination of current law and the specific individual rights and institutional obligations proposed in its other recommendations. For example, the Commission believed that the specific problems concerning erroneous information reported by credit grantors to credit bureaus would be addressed by allowing an individual to be informed of the reasons for an adverse consumer credit decision, and to see, copy, correct, and amend the information used in that decision. While this mechanism would not necessarily prevent an error from occurring, it would adequately protect the individual when an error did occur. The Commission did not believe that preventative protections for accuracy, timeliness, and completeness were necessary in the consumer credit area for records other than those which are disclosed to the authorization services. This option is supported by the Department of Commerce and the National Credit Union Administration. Note that only options 2 and 3 were presented in the review process.

Option 3: No action:

The Treasury Department and industry oppose both the Commission's specific recommendation (Option 2) and the proposal presented in Option 1 above. Card issuers believe that market pressures already force them to have reasonable procedures to ensure accuracy. They believe this is true for all credit records, including those disclosed to the independent authorization systems. The card issuers fear that a legislatively imposed requirement will eventually result in government's dictating the specific procedures that business must follow to ensure accuracy. They point to the FTC suit against Equifax (a major consumer reporting agency) for not having "reasonable procedures to assure maximum possible accuracy" in which the FTC administrative law judge made very specific decisions regarding the procedures that he believed were "reasonable."

Finally, the imposition of a general legal requirement may place a greater burden on smaller credit grantors and retailers, exacerbating an existing trend

toward the disappearance of credit granting by smaller businesses. The Commission recommendation would be less likely to have such an effect because it is directed only to credit-card issuers, which are already predominantly automated and therefore have already included provisions in their systems for maintaining the integrity (i.e., at least the accuracy and timeliness) of their data bases. This option is supported by the Department of the Treasury, which believes that current law provides sufficient protections.

Decision:

_____ Federal law should require a credit grantor to have reasonable procedures to ensure the accuracy, timeliness, and completeness of the information it collects, maintains, and discloses.

_____ Federal law should require that a credit-card issuer adopt reasonable procedures to ensure that the information it discloses to an independent authorization service is accurate at the time of disclosure.

_____ Adopt no new "reasonable procedures" requirement in consumer credit.

C. Commercial Credit Industry

Description of the Record Relationship

Commercial credit is most frequently extended to one business by another, e.g., when a manufacturer sells goods to a buyer with some or all of the payment due sometime after delivery. Commercial credit is also extended to commercial establishments by banking institutions and government agencies, such as the Small Business Administration.

Commercial reporting services, such as Dun & Bradstreet, collect information about businesses and their principals on a regular basis. When a business seeks commercial credit, the credit grantor often requests a report on the business from one of these reporting services. For medium and large companies, commercial credit decisions are generally made on the basis of information about the business entity, rather than about the individual owners and officials. However, for small businesses, such as partnerships and sole proprietorships, personal information may figure extensively in the credit granting decision, and the livelihoods of the owners and principals may be directly affected.

Current Law

Neither the information practices of commercial reporting services nor the use made of their reports is regulated by the Fair Credit Reporting Act, which regulates consumer reporting agencies. However, Federal Reserve Board Regulation B, implementing the Equal Credit Opportunity Act, requires commercial credit grantors, upon request, to notify a credit applicant whose request for credit has been denied of the reasons for the adverse commercial credit decision.

Issues for Decision

With regard to the records about individuals created and maintained by commercial credit grantors and commercial reporting services, the Privacy Commission recommended that Federal law provide:

1) An individual right, upon request, to see, correct, and amend information about him maintained by a commercial credit reporting service;

2) An individual right to be notified, upon request, by a commercial credit grantor who has used a commercial credit report containing personal information on the individual to make an adverse credit decision, of the identity of the commercial credit reporting service that made the report; and

3) enforcement by:

a) an individual right of action, and

b) the Federal Trade Commission for repeated or systematic violations.

The Privacy Commission did not study the commercial credit industry in detail, and, in particular, did not establish a detailed record on the practices of commercial credit grantors. The Department of Commerce supported the Commission's recommendations in the commercial credit area; the Department of the Treasury opposed them. While there is little disagreement with the substance of the above Commission recommendations, the limited record and the strong industry opposition suggest that the primary issue in the commercial credit area is:

1. Should the recommendations of the Privacy Commission (listed above) for the personal records created and maintained by commercial credit grantors and reporting services be adopted in Federal law?

Pro:

Commercial credit reports contain varying kinds of personal information on the owners and managers of businesses which seek commercial credit. This information on a company's principals can be critical to the decision of whether or not to grant credit, particularly for smaller businesses. Under present law, an individual whose business is denied credit because of personal information about him in a commercial report has no legal right to compel the credit grantor or commercial reporting service to disclose the information on which the decision was made, nor can he compel the credit grantor to disclose the name of the commercial reporting service (or even whether one was used). Although the commercial reporting industry will generally voluntarily show reports on a business to the

business' owners and officers, the absence of an explicit legal right to this disclosure can be crucial when there is a dispute and access is denied.

The commercial credit industry argues in opposition to this recommendation that businessmen have the sophistication and market power to protect their own interests without the need and attendant costs of providing these rights by law. However, it is primarily the smaller businesses whose credit worthiness is decided on the basis of personal information about individual managers and owners, and it is exactly these businesses which lack the market power to protect themselves when credit is denied on the basis of inaccurate information. Moreover, the cost of implementing the proposal would be minimal, since the only change required from present practice is that a credit grantor would have to disclose the identity of a commercial reporting service whose report was used to make an adverse credit decision.

Finally, Dun and Bradstreet, the nation's largest commercial reporting service, agrees to the appropriateness of these procedures. However, it believes that only the second requirement is a candidate for Federal action--the marketplace, in its judgment, being a sufficient incentive for the first requirement. Further, it believes that the second requirement should be imposed only through regulations implementing the Equal Credit Opportunity Act, not through new legislation. (The authority of the Federal Reserve Board to expand the ECOA regulations in this manner is unclear.)

Con:

The commercial credit granting and reporting industries oppose privacy measures regarding the personal information they collect and maintain for three primary reasons. First, industry argues that these procedures are consonant with present practice and therefore unnecessary. Second, the commercial reports at issue contain only limited personal information, and most of that information is supplied directly by the subject or taken from public records. The personal information contained in the reports is thus relatively accurate and generally known

to the individuals to whom it pertains. Third, they argue that businessmen are knowledgeable about credit granting and credit reports, and have the sophistication and market power to protect themselves.

As an alternative to legislation at this time, industry suggests that government develop and monitor a code of voluntary standards along the lines of the Commission's recommendations. This would further encourage voluntary action by the industry, and in the event of non-compliance could form the basis for legislation at a later date.

Decision:

_____ Yes, the Privacy Commission recommendations (as listed above) should be adopted in Federal law (using, to the extent possible, the regulations implementing the Equal Credit Opportunity Act and otherwise through a new Federal statute).

_____ No, the Privacy Commission recommendations should not be implemented through legislation, but should be suggested as voluntary standards with legislation to follow in the event of non-compliance.

_____ No, take no action.

2. Should Federal law require that commercial reporting services have reasonable procedures to assure the accuracy, timeliness, and completeness of information pertaining to individuals included in reports produced by them?

For a general discussion of this issue, see "Accuracy, Timeliness and Completeness" in Section I.G.6. above. (Note: Commercial credit grantors rarely, if ever, collect or use personal information about the individuals involved in businesses which seek commercial credit, other than that contained in the reports of a commercial reporting service. Nor do they disclose personal information to these services; they report only ledger information on the credit accounts of the businesses with which they have a credit relationship. For these reasons the Commission did not consider placing a "reasonable procedures" requirement on commercial credit grantors regarding the personal information which they maintain.)

Pro:

Consumer reporting agencies are required by the Fair Credit Reporting Act to have "reasonable procedures" to assure the accuracy of information in their reports, but commercial reporting services are not. The Commission recommended, and the Department of Commerce agreed, that the FCRA should be amended to impose a "reasonable procedures" standard on that part of a commercial reporting service's activities that involve information about individuals.

A requirement that commercial reporting services have an affirmative responsibility to be accurate when initially making a report is important because an inaccurate report about a businessman may cause him to lose a business opportunity that cannot be recaptured when the report is later corrected. For example, a retailer who is unable to replenish his inventory because of an inaccurate credit report will be unable to make up those sales once the report is corrected. It is critical to him that the report be accurate the first time around.

Moreover, the reasonable procedures standard appears to have worked effectively in the consumer reporting field, where it caused significant changes in industry practice. Equifax, which prepares both consumer reports and commercial reports, states that the requirement would pose no additional burden because it follows the same procedures in preparing both kinds of reports. In addition, if the model of the FCRA is used to fashion this requirement, there would be no need for detailed government regulation.

Con:

The Treasury Department and the commercial reporting industry oppose this recommendation. Treasury believes that this protection is adequately provided by the Equal Credit Opportunity Act, the Small Business Act, and other Federal laws. (The ECOA provides that applicants for commercial credit be given the reasons for adverse decisions and the Small Business Act, which governs certain Small Business Administration loan programs, prohibits discrimination in making these loans. Neither act imposes a reasonable procedures standard).

Industry opposes this recommendation out of fear that it would lead to pervasive government regulation of business practices. Second, they assert that the forces of the market place already discourage the reporting of inaccurate information. Finally, industry argues that there has been no showing of harm flowing from present industry procedures.

Decision:

_____ Yes, Federal law should require that commercial reporting services have reasonable procedures to assure the accuracy of information pertaining to individuals included in reports produced by them.

_____ No, such requirements should not be imposed.

D. Depository Institutions

Description of the Record Relationship

Depository institutions -- banks, savings and loan associations, and credit unions -- offer both credit and depository services. To the extent that they make consumer, commercial, and mortgage loans, they are treated as credit grantors in this memorandum. To the extent that they provide checking and savings accounts and, as part of that service, offer check guarantee, or electronic funds transfer privileges, they are treated here as depositories.

Traditionally, the primary deposit services that a depository provides for its non-business customers are checking and savings accounts. To open such an account for an individual, the depository usually requires only a signature and deposit. It rarely conducts an investigation or collects extensive personal information. Once the account is established, however, the records of checks and deposits which the depository compiles can become a virtual economic and social diary for an individual. For this reason, depositories are acutely aware of the concern to keep their client's financial affairs confidential.

This more traditional view of depository institutions and their record systems is being altered, however, by the extension of new services such as "overdraft protection" and the emergence of Electronic Funds Transfer (EFT) systems which combine traditional depository functions (checking and savings) with credit card-type payment mechanisms. These services carry an attendant risk which depositories are willing to accept only after conducting a review of an applicant's credit background. Some depositories and other independent companies are also beginning to offer services which guarantee check payment, thus combining in one institution the more common functions of depositories, credit bureaus, credit authorization systems and insurers. The Privacy Commission recommended a privacy policy designed to address these new functions and the new record systems which will evolve.

Current Law

When a bank grants overdraft privileges, credit cards, or other credit services, it is subject to the Equal

Credit Opportunity Act and must disclose the reasons for an adverse decision if the individual requests. When a depository offers checking and savings services, it is covered by no similar Federal law, or by any other Federal law giving the individual rights to see, copy, correct or amend his records.

In addition to state regulations, depositories are required by Federal law to accumulate certain records and make them available to the government. The Bank Secrecy Act of 1970 and its implementing regulations require depositories to retain copies of checks drawn over $100 (in practice, most depositories copy all checks); the Act also requires banks to report to the government financial transactions over a certain amount.

Although a number of states (notably California) have legally enforceable confidentiality standards for financial records, the 1976 Supreme Court decision in United States v. Miller makes it clear that under Federal law account records are business records of the bank, and the account holder has no "expectation of privacy" in them. He thus cannot object to their disclosure on Fourth Amendment grounds.

Areas of Agreement

There is agreement among the Privacy Commission, the Department of Commerce, and significant segments of the banking industry that, with regard to depository institutions, Federal law should require:

a) that depository institutions notify applicants of their collection and disclosure practices, and follow that notice;

b) that depository institutions promptly notify independent check-guarantee and check authorization services of corrections of erroneous information previously reported to them;

c) that check-guarantee and check-authorization services be subject to the provisions of the Fair Credit Reporting Act;

d) a legally enforceable expectation of confidentiality (as defined in Section I.G.7.); and

e) enforcement by:

(i) an individual right of action, and

(ii) the FTC or other depository institution regulatory agencies for repeated or systematic violations.

Areas of Disagreement

1. Should an individual have the right to be given the specific reasons for an adverse depository decision and to be informed of the specific item(s) of information used in making that decision?

Pro:

The Commission recommended this provision, and Commerce and Treasury support it. They believe that depository and credit institutions should be treated alike. Although it is rare, individuals sometimes are turned down for a depository or checking account, for example, on the basis of negative information received from a check authorization service. In this instance, the Commission asserted that the individual should be able to know this and to see the item(s) of information used by the bank in making that decision.

The Federal Reserve Board has suggested that, if the Commission's recommendation is adopted, the term "adverse decision" be narrowly defined (e.g., so as not to include the declination of a specific transaction). This way the proposed requirement would not create much of a burden.

Con:

If there is a decision to deny a loan, overdraft privileges, or a credit card, the Equal Credit Opportunity Act currently requires a depository to inform the individual of the reasons. Depositories claim that there is no need to apply this requirement to opening a deposit account since they almost never deny an application. They assert that it would be costly and unnecessary to set out the item(s) of information that support the adverse decision.

The Federal Deposit Insurance Corporation (FDIC) opposes applying this or any other privacy requirement

to depositories absent a showing of abuse.

Decision:

_____ Yes, require disclosure of the reasons for an adverse depository decision and, upon request, the items of information used in making the decision.

_____ No.

2. Should an individual have a right to see and copy at any time all reasonably retrievable records about him held by a depository, not just the items of information used to make an adverse decision?

Pro:

To provide for access only to depository records used in making an adverse decision is inconsistent with the approach the Commission took in other areas (such as insurance). Credit grantors, landlords, and others often seek information about an individual from his bank, and the individual should arguably be able to avoid an adverse decision in these areas by correcting erroneous information before a disclosure or decision is made. He can do so only if he has a general right to see and copy these records at any time.

Con:

The Privacy Commission opposed giving the individual a right to see and copy these records at any time because it believed that it would place an unnecessary burden on depositories. The individual presently receives copies of records with respect to his depository account on a periodic basis, usually in the form of monthly statements, cancelled checks, and receipts for deposits and withdrawls. The Commission believed that the individual's right of access is important only in the adverse decision situation, where the individual may be affected by information that does not stem from transactions for which he already has records. The responding agencies have not spoken directly to this issue.

Decision:

_____ Yes, the individual should have a right of access to all depository records upon request.

_____ No, an individual right of access to depository records should be limited to those records that have been used to make an adverse decision about him.

E. Insurance Industry

Description of the Record Relationship

Two of every three Americans have some form of life insurance; 90% of the civilian population under age 65 have some form of individual or group health insurance; and 15% of all Americans are covered by one of the pension plans offered by life insurance companies. Unlike the credit area, in which eligibility decisions increasingly are based on objective criteria, insurance decisions continue to reflect the insurance underwriter's subjective evaluation of the individual applicant.

The insurance industry uses highly personal records extensively in its decision making. For health and life insurance, the primary risk factors are current health, employment, and hobbies, e.g., sky diving, auto racing, etc. For property and casualty insurance, more subjective criteria, such as prior claims history, driving habits, and "moral life-style information," are added to these factors.

Insurance companies also collect a great deal of information about individuals in the course of settling claims. Some of this information may be used in evaluating an individual's subsequent insurance application. This is especially true of property and casualty insurance, where the paramount concerns are preventing fraud and the accurate prediction of risk.

Within the insurance industry, a variety of support organizations have arisen which facilitate the collection and sharing of personal information for use within the industry. In addition to consumer reporting agencies, which conduct investigations on individuals for underwriting purposes, organizations such as the Medical Information Bureau (MIB) index personal information on policy holders and applicants for use by subscriber companies.

Current Law

Traditionally, the insurance industry has been regulated at the state level. With regard to information practices, some states, notably California, have tried to regulate companies' use of certain information, e.g., moral life style, on the basis of propriety and relevance. Other states have proscribed the use of age, race, and sex. The consumer reporting industry, which investigates

individuals for insurers as well as other clients, has been regulated at the national level by the Fair Credit Reporting Act since 1970. There is, however, some doubt whether organizations like the Medical Information Bureau (MIB) are covered by this law. As for the insurance companies themselves, no Federal legal controls exist with regard to the accuracy, timeliness, and completeness of the information they collect and maintain.

Partially in response to the Commission's report, some state insurance commissioners have begun to develop fair information practice codes for the insurance companies operating within their states, and the National Association of (State) Insurance Commissioners has drafted model state legislation incorporating the bulk of the Commission's recommendations. One state (Virginia) has a recently enacted law requiring the consumer to be notified of the reason for an adverse insurance decision.

Areas of Agreement

Although there is disagreement about how privacy protection in the insurance industry be implemented, the Commission, the Department of Commerce, and some insurance companies, particularly in the life and health areas, agree that substantive protections should include:

a) a requirement that insurance institutions notify applicants of their collection and disclosure practices, and follow that notice;

b) the right for an individual to challenge the accuracy of those insurance records to which he has access (as defined below);

c) a requirement that the record keeper send any corrections it makes of inaccurate information to:

   i) anyone designated by the inividual who has received the inaccurate information within the preceeding two years;

   ii) any support organization which regularly receives such information; and

   iii) any support organization which furnished the inaccurate information;

d) a prohibition on pretext interviews, (an interview in which an investigator: (1) pretends to be someone he is not; (2) pretends to represent someone he does not; or (3) misrepresents the purpose of the interview);

e) the right for an individual to be given the reason(s) and item(s) of information used in an adverse insurance decision;

f) the right for an individual not to be denied insurance based solely on the fact that he previously has been denied insurance; and

g) a legally enforceable expectation of confidentiality (as defined in Section I.G.7).

Areas of Disagreement

1. Should the privacy protections applicable to the insurance industry be required by Federal law?

Pro:

The Commission, the Department of Commerce, and some insurance companies, particularly in the life and health areas, agree that some uniform Federal privacy standards are desirable in the insurance area so that a person's minimum rights would be the same throughout the country. There is no widespread state regulation of insurance information practices and it is not clear that states are interested in such comprehensive regulation at this time. In the case of insurance application forms, which states traditionally have regulated, the Commission did, however, deem it appropriate to leave regulation to the states. The extent and effectiveness of voluntary action by the insurance industry are uncertain at this point.

Con:

Some life and health insurance companies and most casualty insurers, with two major exceptions, believe that implementation of the Commission's recommendations should be left to the states. The general policy of the Federal government, embodied in the McCarran-Ferguson Act of 1945, has been to leave regulation of insurance to the states (although aspects of the general Federal-state regulation of insurance question are currently

being examined by OMB). The companies' position is based more on their desire to maintain the existing regulatory framework than on any particular privacy issue. As they currently operate under 50 different state regulatory schemes, many companies see no objection to differing privacy regulations.

Decision:

_____ Yes, privacy protections applicable to the insurance industry should be required by Federal law.

_____ No, regulation of the insurance industry's privacy practices should be left to the states.

With regard to individual access to records, there is agreement that third party claimants, i.e. those who are neither policy holders nor beneficiaries, should not have a right of access to insurance claims records and that the identity of non-institutional sources of information (for instance, a neighbor or associate) need not be revealed where information was provided on the condition of confidentiality. In addition, there is agreement that a statutory provision governing individual access to insurance records should include a qualified privilege such that an individual would have no right of action for defamation against a company that was neither negligently nor willfully defamatory. Moreover, it is agreed that the Fair Credit Reporting Act, which provides the individual the right to know the "nature and substance" of a consumer investigative report, be amended to allow him to see and copy that record.

There is, however, opposition within the insurance industry to the Commission's general recommendation that individuals should have a statutory right to see and copy their records. Although major elements of the industry publically support the policy of individual access to insurance records, there are two areas of contention. First, some base their support for the Commission's recommendation on an assumption that the recommendation would allow the information used in making underwriting decisions to be excluded from the records to which the individual is allowed access. The Commission provided--although arguably not in explicit language--that a right to see and copy insurance records must include underwriting records, since they contain most of the personal information of critical importance

to the decision of whether or not to insure an individual and at what rate. For this reason, the question of individual access to underwriting records is not raised for separate decision, but rather subsumed explicitly into the larger issue of individual access to records. The second area of contention concerns individual access to first-party claims records (records of claims made by an individual to his own insurer). These questions are raised for decision below.

2. Should an individual have a right to see and copy the records about him maintained by an insurance institution, including information used by an insurer in making an underwriting decision?

Pro:

Individual access to records is a precondition to several of the other basic elements of privacy. It enables the individual to check whether the records contain information beyond the scope of the prior collection notice and to challenge the accuracy of information contained in the records. Moreover, the information used by an insurance company in making its underwriting decisions is exactly the information of concern to the individual. Without such access, the general right would be rendered meaningless. Also, with a Federal statute limiting the insurer's liability as a result of disclosure, allowing the individual access to records about him will not be costly in terms of adminstrative procedures or litigation. This is the Privacy Commission recommendation, and is supported by the Commerce Department.

Con:

Insurance industry opposition to the individual's right to see and copy insurance records comes primarily from property and casulty insurers and focuses on the records used in their underwriting decisions. They believe that these records represent the subjective views and opinions of their professional underwriters concerning the business judgement of accepting a particular risk. In addition, they regard these records as a work product, since they are not disclosed outside the company. To allow the individual direct access to these records would, they assert, restrict the ability of the underwriter to take all available information into account in his decision.

Decision:

_____ Yes, an individual should be able to see and copy the records about him maintained by an insurance institution, including the records used in making underwriting decisions.

_____ No, an individual should have no such right of access.

3. Should an individual's right to see and copy the records maintained by an insurance institution include first-party claims records?

Pro:

The Privacy Commission considered specifically whether an individual should have a right to see and copy first-party claims records, and recommended that he should. The Department of Commerce concurs. These records are not only important to the individual with regard to a particular claim, but once the claim is settled they can affect whether or not he will be able to get insurance in the future and at what rate. This is particularly true with property and casualty insurance where a record of prior claims is the most important factor in making these decisions. Although these records are generally available to the individual as a result of civil procedure in the context of litigation, the Commission believed that the individual should be able to see and copy them, upon request, since most cases do not go to litigation and claims records may subsequently be used in underwriting. However, to ensure that the settlement procedures not be compromised, the Commission recommended that access not be allowed until the claim is settled.

Con:

Important elements of the insurance industry oppose allowing an individual to see and copy first-party claims records, even after the claim is settled, because they believe that these records represent an adversary relationship between the individual and the company. They fear that forcing this information to be disclosed will make insurers reluctant in the future to settle a claim if the

records show that settlements are made with claimants who may not be legally entitled to a settlement. They argue that allowing the individual access to a claims record after the claim is settled will not prevent him from reopening the claim based upon the information in the record. The insurance industry believes that the individual is already well protected in court regarding access to these records.

Decision:

_____ Yes, an individual should be able to see and copy first-party claims records maintained by an insurance institution.

_____ No, an individual should not have a statutory right to see and copy first-party claims records, independent of court action.

4. Should an individual's right of access to his insurance records in the hands of an insurance company or support organization include access to information prepared by another institutional source, e.g., a consumer investigative report maintained by an insurance company?

Pro:

The Commission and the Department of Commerce support this proposal. The insurance company makes the decision to grant insurance, and at what rate. Therefore, it is the insurance company's records which are important to the individual. As noted earlier, the Fair Credit Reporting Act now allows the individual to know the "nature and substance" of a consumer investigative report, but does not require that the insurance company itself make that disclosure. In fact, most contracts between insurance companies and consumer reporting agencies prohibit the insurance company from disclosing the report to the consumer.

The individual has a market relationship only with the insurance company. To require the individual to seek out the institutional source will discourage many people from exercising the right of access. Finally, while the institutional source can explain the information in the report, it cannot explain the information's meaning to the insurance

A number of major insurance companies support this proposal. Others do not. The cost to the industry would be slight, and the industry has an interest in having accurate information available to it.

Con:

Some insurance companies and the major consumer reporting agencies oppose this proposal. They argue that the consumer reporting agencies alone are competent to discuss their reports' contents with the individual. They claim that allowing an insurance company to discuss a report with the individual could lead to misunderstandings and might inhibit the correction process (if the report contains inaccurate information). Some insurance companies claim that this proposal would impose additional costs on them to train their staff to discuss such reports with people.

Decision:

_____ Yes, an individual's right of access to his insurance records should include access to information originating with another institutional source.

_____ No, information originating with another institutional source should be excluded from an individual's right of access to his records in the hands of a recipient record keeper.

5. Should there be a mechanism for the individual to challenge the relevance and propriety of information collected or used by an insurer or insurance support organization?

The Commission recommended that each State Insurance Commissioner collect complaints concerning the relevance and propriety of the information collected and used by insurance institutions, and either promulgate rules or recommend state legislation to proscribe the collection of irrelevant or improper information. In addition, the Commission suggested that the Federal Insurance Administrator could be given the authority to compile reports from individual consumers and from the states, and report to the Congress concerning the need for legislation. It did not recommend, however, that the

Federal Insurance Administrator have the rule-making authority urged for State Insurance Commissioners. The decision as to the role of these government agencies will be made below.

Pro:

The Commission and the Department of Commerce support this proposal. When they apply for insurance, individuals may be frustrated by what they believe to be overbroad and irrelevant or improper requests for information. Generally, they do not have the market power to prevent its collection; the alternative is to forego entirely the benefit of insurance. A government agency, such as the office of a State Insurance Commissioner, could consider consumer complaints and take action or suggest remedial legislation on a case-by-case basis. Such a mechanism already exists in California, where action has been taken to proscribe the collection of "moral life-style" information for use in insurance decisions

Con:

The insurance and consumer reporting industries uniformly and vehemently oppose this recommendation. They believe that the marketplace discourages the collection of irrelevant or improper information, and that there is currently a trend in sections of the insurance industry to collect less information. Industry argues that most information is relevant to some business purpose, and does not want government interference in business decisions about what information to collect. These same arguments were used by these industries to remove general relevancy requirements which had been included in the original draft of the Fair Credit Reporting Act.

Decision:

_____ Create a Federal governmental mechanism (using the Federal Insurance Administrator or other Federal entity), and urge the states to create state governmental mechanisms, for the individual to challenge the relevance and propriety of information collected and used by insurance institutions.

_____ Urge the states to create governmental mechanisms for the individual to challenge the relevance and propriety of information collected and used by insurance institutions.

_____ No such mechanisms should be created.

6. Should Federal law require insurance institutions to adopt reasonable procedures to ensure the accuracy, timeliness, and completeness of the information it collects, maintains, or discloses about an individual?

For a general discussion of this issue see "Accuracy, Timeliness, and Completeness" in Section I.G.6 above.

Pro:

It is the position of the staff of the Federal Trade Commission that a general "reasonable procedures" standard similar to that contained in the Fair Credit Reporting Act is a necessary component of any comprehensive privacy policy in the insurance area. The other Federal agencies have not directly addressed this issue.

The FTC staff asserts that the specific privacy rights and requirements proposed by the Commission would not effectively prevent erroneous information from circulating within the insurance industry and from being used to make adverse decisions about the individuals to whom it pertains. On the other hand, a legal requirement that an insurer take reasonable steps to ensure the accuracy, timeliness, and completeness of its information might, for instance, encourage a reinvestigation of information, or perhaps prompt the insurer to ask the applicant to explain or document information before using it to make a decision. The specific procedural rights and requirements proposed by

the Commission would not, if adopted, fully address such a problem, and this argues in favor of a general standard.

The FTC staff also believes that a general requirement for accuracy, timeliness, and completeness would be preferable to the Commission's approach of establishing procedural rights for the individual and placing specific requirements on flows of information within the insurance industry. They argue that these requirements are inflexible, and would not allow an insurance company, for example, to institute alternative procedures which might better achieve the objectives of accuracy, timeliness, and completeness, or address problems developing in the future. Placing a general requirement on the record keeper would ensure that the objectives of accuracy, timeliness, and completeness are given sufficient consideration when decisions are made about how to process and maintain personal information.

Finally, the FTC staff asserts that placing this requirement on insurers would erase an often artificial distinction which the Fair Credit Reporting Act currently draws between consumer reporting agencies and insurance institutions. The FCRA currently places a "reasonable procedures" requirement on consumer reporting agencies, while an insurer, which uses the reports they produce or which may conduct similar investigations itself, is not covered.

Con:

The Commission explicitly recommended that insurance institutions not be required by statute to adopt reasonable procedures to ensure the accuracy, timeliness, and completeness of its records, but rather adopt such practices voluntarily. The Commission believed that the mix of specific individual rights and institutional obligations it recommended will assure the kind of management attention to record-keeping policy and practice that achieves accuracy, timeliness, and completeness and, morever, that such rights and obligations were sufficient to address this problem.

This proposal is also strongly opposed by the insurance industry, which fears extensive government regulation of the information used to make business

decisions. Industry believes that the marketplace is the best vehicle for establishing the balance between the cost and the degree of accuracy, timeliness, and completeness of recorded information. It is convinced that the vagueness of a general standard would lead to needless compliance costs, and the industry would prefer the other specific procedural requirements whose costs could be more easily anticipated.

Decision:

_____ Yes, insurance institutions should be required to adopt reasonable procedures to ensure the accuracy, timeliness, and completeness of the information they collect, maintain, or disclose about an individual.

_____ No, there should be no such statutory requirement.

F. Employment Records

Description of the Record Relationship

Employment records may be the most extensive category of personal records maintained about individuals in our society. Private employers require applicants and employees to supply detailed information about their lives, to submit to tests and examinations, and to authorize the employer to acquire whatever records it wants about them from other organizations. In addition, as a result of providing various job benefits and services, employers frequently maintain extensive medical and insurance records on their employees. There is, moreover, a growing trend among larger employers toward the computerization of personnel files. Thus, these records may be immediately available to different levels of management and at various job sites around the world.

This trend toward more sophisicated and detailed record keeping is balanced, in part, by increasing tendencies for private employers to allow employees access to at least a portion of their records, and to extend employees the opportunity to correct inaccuracies. Employers are also more reluctant to disclose information about their employees than before, although it is unclear whether employers with these policies effectively limit access by law enforcement and other government officials.

Current Law and Practice

The maintenance and enforcement of privacy protection with respect to employment records presents special problems. Except as covered by collective bargaining, there is no general legal framework in the private sector employment environment which could accommodate the resolution of privacy questions, such as what records are covered or whether the use of particular information in an employment decision is improper or irrelevant. It would, for example, be relatively simple for an employer to terminate or fail to promote an employee who complains that his privacy is being invaded, and because of the multitude of factors involved in any employment decision -- both business-related and personal -- it would be difficult for the employee to prove that such an action was retaliatory. In addition, consistent regulation is difficult because of the vast differences among employers with regard to size, type of employees, benefits provided, centralization of work place and record-keeping functions, nature of

promotion and other personnel programs, and degree of unionization.

There are two large groups of employees to whom some elements of a basic privacy policy now apply in law: Federal government employees and private employees covered by collective bargaining agreements. Both have evolved from, and are enforced through, a system of established due process, which stipulates that the employee may be discharged only for just cause. Privacy protections for Federal employees are also provided by the Privacy Act of 1974, which gives the employee access to his records even without his filing a grievance or complaint with the Civil Service Commission.

The privacy rights gained by non-Federal employees as a result of collective bargaining contracts are more limited than those accorded Federal employees and differ from contract to contract. When an employee files a grievance, the union and the employee are generally allowed access to the relevant employer records for use in the proceeding. Knowing this, many employers carefully limit the potentially sensitive information in the personnel files of union employees. In addition, three states have recently passed laws allowing employees to see and copy their records. Over two-thirds of all private sector employees, however, do not have any of the above protections.

In addition, the Fair Credit Reporting Act allows employees access to investigative reports and other types of consumer reports prepared for employment decisions. However, just as with consumer reports prepared for insurers and credit grantors, this is a limited right which does not apply where the employer conducts his own investigation.

Areas of Agreement

There is agreement among the Privacy Commission, the Department of Labor, and private employers that privacy protection in private sector employment should include:

a) an employer's notice to his employees of the collection and disclosure practices;

b) an opportunity for the individual to see and copy the records maintained by his employer;

c) an opportunity for the individual to correct and amend his records;

d) a limitation on disclosure to that contained in the notice;

e) a prohibition on pretext interviews (an interview in which an investigator: (1) pretends to be someone he is not; (2) pretends to represent someone he does not; or (3) misrepresents the purpose of the interview); and

f) that for the job-related records which an employer maintains, the above principles should be endorsed by the government but made voluntary, not mandatory, on the part of the employer.

Areas of Disagreement

There is a need for decision in the employment area on the following two questions, which go beyond the above noted areas of concensus and would implement by statute some of these measures.

1. Should there be a Federal law granting employees the right to see and copy the personal records which their employer maintains about them?

Note: It is generally agreed that any law which grants employees a right to see and copy the personal records maintained about them by their employer must exclude certain records from those to which the employee is given a right of access. This memorandum does not attempt to precisely distinguish those records which the employee would not be allowed to see and copy; however, such records might include: (1) industry security and claims records; (2) records of supervisory estimates of promotion potential, company promotion planning, or plans for future assignments or salary adjustments; and (3) records obtained from third parties under a pledge of confidentiality.

Pro:

There is increasing interest in employee rights issues, including privacy. The enactment of a law granting employees the right to see and copy records would be an important first step in this direction, even though such a law, absent a right to challenge the accuracy of records and a strong enforcement mechanism, may not create an enforceable

right for all employees in every situation. Where the employees are union members, this right would enable them to see records outside of the grievance process. If the records were incorrect or improper, then this itself might become the subject of a grievance proceeding.

A few states have enacted laws granting employees these rights, although they do not provide for consistent procedures and penalties. For large corporations, operating in many states, proliferation of such laws could create substantial administrative problems. A Federal law with uniform procedures and penalties would be more efficient and effective.

Con:

Many employers are already moving voluntarily to provide employees with an opportunity to see and even correct their records. In addition, the Commission recommended voluntary implementation in employment because it believed that, absent a strong enforcement mechanism, employees would be unable to assert their rights without fear of retaliation, subtle or direct, by employers. The right to see and copy records, by itself, without a right to challenge their accuracy and a strong enforcement mechanism, is a mere shadow of a right; and, to give employees the power to effectively enforce such a right would fundamentally change the nature of the employment relationship in this country (as discussed more fully in the Con to the next question for decision).

The Commission found that the two existing state statutes are not frequently used by employees, and their enforcement has been virtually non-existent. Furthermore, the activity to date at the state level (three states now have some variety of "see and copy" laws) does not indicate a sufficient trend to justify a Federal statute. The Department of Labor supports this position.

Decision:

_____ Yes, there should be a Federal law granting employees the right to see and copy the personnel records their employer maintains about them.

_____ No, employee access to employment records should be sought through voluntary action on the part of employers.

2. Should there be a legally enforceable expectation of confidentiality (as defined in Section I.G.7) for employment records?

Pro:

Employment records are frequently the first place to which investigators and other outside parties go when seeking information about an individual. Under current law, employers can disclose as they please. This problem of privacy protection in the employment context is more amenable than any other to individual enforcement through court action. Requests for information and disclosures by employers can be documented. It would therefore be relatively easy for an employee to substantiate improper disclosure. Moreover, under ordinary circumstances many employers already release information from employee files only at the request of the employee or pursuant to a legal requirement. It would therefore not impede their existing business arrangements in any significant way.

Con:

Most disclosures of personal information made by employers are at the direct request of, and in the interests of, their employees, usually for such purposes as obtaining credit, a lease, or subsequent employment with another organization. If an enforceable expectation of confidentiality is created for these records, employers will have to develop systems of accountability so that disclosures are made only with the specific authorization of the employee, and they will be liable for improper disclosures. Given the cost of both of these factors, employers might not be inclined to disclose information about their employees to others, even at the specific request of the employee.

In addition, even if an employee were to win a law suit against an employer for improper disclosure, it would be difficult to protect him from the more subtle forms of employer retaliation, such as failing to promote him or giving him undesireable work assignments. Indeed, it might even be impossible to protect such an employee from termination. Furthermore, if a provision were added prohibiting employer retaliation, there is still the question of how long the employer would be required to retain an employee who has sued him before he would not have to show that a dismissal was non-retaliatory. A heavy burden would be placed on a private employer to establish the legitimacy of its decision to fire an employee, in effect giving employees who sue a presumptive right to a particular job. There is also a question of who would evaluate such a showing by the employer and what standards they would use.

Finally, the tremendous diversity in the sorts of business carried on by private employers is reflected in an equal diversity of information disclosure needs and practices. Currently, a great deal of information about employees flows informally to ensure the propriety of employee conduct or to verify background information in hiring or promoting to sensitive positions. It can be argued that no sweeping prohibitions on employer disclosures should be established unless and until the pattern of flows in different businesses is understood and provisions are made to accomodate those which are proper.

Decision:

_____ Yes, there should be a legally enforceable expectation of confidentiality for employment records.

_____ No, employers should limit their disclosures of information on employees through voluntary action.

3. Should the Department of Labor develop a voluntary code of conduct for those privacy measures recommended for voluntary adoption in employment, and monitor compliance with that code?

Pro:

The Privacy Commission found that most employers were almost totally unaware of privacy issues until quite recently. It can be argued, therefore, that they are ill-equipped to design new record-keeping policies and practices without outside, expert guidance. Centralization of this effort in the Department of Labor will ensure consistency and will enable the government department most concerned with the problems of the work force to exert its influence on employers. This channel has been used before, and, according to the Department of Labor, employers have responded affirmatively. A government monitoring effort would further encourage employers to follow through on voluntary compliance.

Con:

Although employers have only recently become active on privacy issues, large private sector corporations have been responding affirmatively since the Commission issued its report. A voluntary code developed by the Department of Labor is not needed at this time.

Decision:

_____ Yes, the Department of Labor should develop a voluntary privacy code for employers and monitor their compliance.

_____ Yes, the Department of Labor should develop a voluntary privacy code for employers, but should not monitor their compliance.

_____ No, the Department of Labor should not develop such a code.

## G. Medical Records

### Description of the Record Relationship

Patients expect doctors to question them closely about all aspects of life in order to make a correct diagnosis and to prescribe the proper course of treatment. Thus, in the medical-care context, questions about the relevance and propriety of the information gathered are rarely raised. Rather, privacy concerns focus upon the patient's access to his own medical record, his ability to challenge its accuracy, and the confidentiality with which it is held.

Today medical-record information is frequently disclosed to institutions other than medical-care providers for use in many non-medical decisions. Often an individual's job or ability to collect on an insurance policy depend on medical-record information being available to the decision-maker. Yet, it is rare for the individual himself to have access to his medical records or to information gleaned from them. One reason is the general reluctance of medical-care professionals to share these records, and another reason is that, legally, medical records belong to the medical-care provider.

### Current Law

Historically, a patient's expectation that information given a doctor will be kept in confidence has been founded on the doctor's adherence to the Hippocratic Oath. In practice, society frequently requires doctors to depart from their oath.

Although 19 states have laws which in some way recognize the confidentiality of medical records, and a doctor can lose his license to practice in 21 states for revealing patient information, few courts allow a patient to sue his doctor for disclosing information about him without his permission. Case law permits doctors almost unlimited discretion in deciding what disclosures to make of patient information.

### Areas of Agreement

The Commission, the responding agencies, and the medical community agree that a Federal law to establish privacy protections for medical records is needed. Such protections would include:

a) the right for an individual to have direct access to the medical records about him (i.e., to see and copy those records), except when the medical professional responsible for the record believes direct access to it might harm the patient, in which case access should be permitted through a designated intermediary;

b) the right for an individual to challenge the accuracy of his medical records;

c) a legally enforceable expectation of confidentiality (as defined in Section I.G.7); and

d) authorizing the Secretary of HEW to issue implementing regulations, and encouraging the states to adopt similar legislation governing medical record keepers not subject to Federal law.

Issue for Decision

The Department of Health, Education, and Welfare has drafted legislation implementing the above principles of privacy protection for medical records, and this proposed legislation has been circulated for agency comment through OMB's legislative clearance process. Agencies that have not received copies should contact OMB. Any agency concerns may be resolved through the OMB process, or, if necessary, should be raised for inclusion in this Presidential Review Process.

H. Education Records

Description of the Record Relationship

Student life produces many records. There are teacher evaluations of academic ability, academic accomplishment, and social adjustment. Applying to private schools and universities largely is a paper process. With regard to the records of educational institutions, most of the protections discussed earlier as basic elements of a privacy policy now are provided by law.

Current Law

The Family Education Rights and Privacy Act of 1974 (FERPA) gives students over 18 and parents of minor students the rights to have access to their records and to challenge the accuracy of their records. FERPA also contains stringent protections for the confidentiality of student records.

Areas of Agreement

The Commission and the Department of Health, Education, and Welfare agree that, beyond the current provisions of FERPA, there is a need for:

a) greater student involvement in developing privacy policies to comply with FERPA, and greater community involvement in the case of public school systems; and

b) an explicit statutory right of action for the individual against any educational institution which fails to comply with FERPA to the detriment of a student or parent.

Areas of Disagreement

1. Should FERPA be extended to cover applicants for admission to schools and colleges, and to educational testing and data-assembly services?

Pro:

The Family Education Rights and Privacy Act now applies only after an applicant is admitted to an educational institution, and at this time he becomes entitled to see his admissions file.

However, unsuccessful applicants for admission are not entitled under FERPA to see the records used in the admission process. In addition, the records of organizations like the Educational Testing Service which administer standardized tests (e.g., the Scholastic Aptitude Tests used for admissions to most American colleges and universities) to thousands of students and assemble academic data about applicants for admission to colleges and universities are not covered by FERPA. The Commission recommended that these exceptions be eliminated.

The Commission did not intend to lay bare the admissions process, and did not believe its recommendations would do so. Rather, the recommendations aim at ensuring that applicants may see and copy these records to ensure that they are judged on the basis of information that is accurate, complete, relevant, and timely.

Con:

DHEW and the university community oppose this recommendation on the basis that it would be costly and administratively burdensome. They do not feel that there has been a sufficient demonstration of need for this extension of FERPA. Since applicants may come from across the country, institutions fear the administrative cost of verifying the identity of the requester and copying and mailing the records. In addition, in most cases, the number of applicants greatly exceeds the number of places available, and decisions are often comparative and most subjective. Therefore, allowing access will be of little use to the applicant who had not been admitted, particularly since it is unlikely that the institution can reconsider its decision if it proves to have been based on inaccurate information.

Decision:

_____ yes, extend FERPA to cover applicants for admission, and educational testing and data-assembly services

_____ no, do not extend FERPA to applicants for admission, and educational testing and data-assembly services.

2. Should FERPA be amended to provide that the student or his parent may not waive his right to see and copy letters of recommendation?

Pro:

FERPA currently permits students and parents to waive any of the rights it grants. The Commission was concerned that students have been coerced into waiving their right of access to letters of recommendation in response to institutional "requests" for waivers. The Commission also developed evidence that educational institutions tend to discount letters of recommendation about students who have not waived their right to see these letters, even though the institution may not know whether the student has actually seen the letters. Finally, without access, a student cannot ensure that information about him supplied by others is correct.

As to the teacher's concerns, the Commission believed that making candid professional evaluations is part of his professional resonsibility. A teacher who makes student evaluations without malice and as part of his official duties is not susceptible to a defamation suit nor, in the Commission's opinion, to any significant threat of physical reprisal from irate students.

Con:

According to DHEW and many students who have dealt with DHEW's FERPA staff, teachers have refused to provide letters of recommendation without assurances of confidentiality. Many educators regard letters of recommendation as private communication and thus view keeping them confidential as a professional perogative. Many educational institutions fear that openness would make letters less candid, and therefore of significantly less value in the admissions process. Moreover, since the student asks the teacher for a recommendation, they argue that the student should be able to waive his right to see it. DHEW supports this position.

Decision:

_____ Yes, FERPA should be amended to provide that the student or his parent may not waive his right to see and copy letters of recommendation.

_____ No, FERPA should not be so amended.

3. Should Federal law (FERPA) be amended to require educational institutions to adopt reasonable procedures to ensure the accuracy, timeliness, and completeness of the records they collect and maintain?

For a general discussion of this issue see "Accuracy, Timeliness, and Completeness" in Section I.G.6 above.

Pro:

The Commission recommended this requirement because it believed that levying responsibility for the content and quality of records on educational institutions would reduce the collection and maintenance of erroneous, incomplete, or misleading information. The Commission found evidence that the accuracy and completeness of records is a significant problem for educational institutions, especially elementary and secondary schools. While it recognized a lack of consensus about the need for these standards and what the standards should be, the Commission believed that they are necessary for "effective educational service delivery and protection of the individual." The Commission believed that the law should establish minimum requirements in this area.

Con:

DHEW opposes the Commission recommendation. It believes that establishment of such procedures should be left to states and localities, many of which already have standards for the content and accuracy of education records. HEW argues that it would be difficult to enforce compliance with a Federal requirement without allocation of substantial additional resources. However, if abuses occur in the future indicating the need for additional safeguards, DHEW believes that new requirements can be established through regulation under the FERPA as currently enacted.

Decision:

_____ Yes, FERPA should be amended to require educational institutions to adopt reasonable procedures to ensure the accuracy, timeliness, and completeness of the records they collect and maintain.

_____ No.

## I. Public Assistance and Social Service Records

### Description of the Record Relationship

Public assistance and social services involve relationships between individuals and state and local governments. Included are programs which provide cash and in-kind benefits to people on the basis of financial need. While most of these programs receive substantial Federal financial support, state and local government agencies are responsible for their administration.

The Commission found that administration of the "welfare system" depends heavily upon the collection and use of personal information. Those seeking assistance generally must disclose sensitive personal information in applying for aid, and they must submit to what can be an extensive verification process. The relationship between the applicant and program administrator is invariably documented in record form. In view of the sensitive nature of the information contained in public assistance and social service records and the need to use that information in making decisions about particular people and about general program funding and priorities, concern for the confidentiality accorded such records presents special problems.

### Current Law and Practice

No overall policy exists with regard to the information practices of public assistance and social service agencies. The Federal government has not required programs receiving Federal funds to adopt the principles of privacy protection in their record-keeping systems. Nor have state and local governments acted independently. In most cases, there are neither guidelines for the accuracy, completeness, relevance, and timeliness of records, nor procedures whereby an individual can challenge the accuracy of records. In some cases, there are no record-keeping requirements at all.

### Areas of Agreement

The Commission and the responding agencies agree that privacy protection for public assistance and social service records should include:

a) a requirement that applicants be notified of public assistance and social service programs'

collection and disclosure practices, and that the notice be followed;

b) the right for an individual to have access to his records, except for:

i) records being used in an ongoing investigation of suspected violations of law by the individual;

ii) medical information, in certain situations as defined in Section II.G, above; and

iii) the identity of sources of information who request confidentiality, and then only when the source's information is not the sole basis for an adverse decision;

c) the right of an individual to challenge the accuracy of his records; and

d) a legally enforceable expectation of confidentiality (as defined in Section I.G.7).

Areas of Disagreement

1. Should an applicant for public assistance and social service programs be able to prevent an agency from obtaining and using information from sources other than himself (i.e., a collateral source) without his consent by requiring the agency to notify him any time it desires to contact a collateral source and allowing him to withdraw his application if he does not want the source to be contacted?

Pro:

Except in a very few states, applicants for, and recipients of, public assistance and social services now have no control over the sources contacted by agencies to verify information. The Commission firmly believed that it was desirable and necessary that agencies be permitted to contact collateral sources only with an individual's consent. Individuals have reason to fear the loss of employment and residence if certain people (e.g., employers and landlords) learn that they have applied for, or are receiving, public assistance or social services. Even people who do not fear adverse

consequences may simply not wish certain people to know of their involvement with public assistance and social service programs.

The Commission recommended that individuals be able to prevent an agency from contacting a collateral source to which they objected by withdrawing their application, except when the individual was suspected of violating a law in connection with a public assistance or social service program. The Commission believed that Oregon and Tennessee's experience with such provisions indicates they can be implemented without significant cost or difficulty. This position has the support of DHEW and the Department of Labor.

Con:

Opposition to the proposal centers on three arguments. First, that "everybody knows who's on welfare," so that the protection would be meaningless in that respect. Second, since the client who needs the assistance can ill afford to forego the benefits, his choice is hollow. Finally, the Commission's recommendation is said to be cumbersome, time-consuming, and expensive. Since the individual is to be given veto rights as to each collateral source, he must be notified whenever the agency wants to make such a contact. Moreover, there is some fear that he might contact the collateral source first in order to try to influence that source to provide information favorable to him.

Decision:

_____ Yes, an applicant should be able to prevent an agency from contacting collateral sources without his consent by withdrawing his application.

_____ No, an applicant should not be able to prevent an agency from contacting collateral sources.

2. Should privacy protections in the area of public assistance and social service programs be implemented by a Federal law setting forth general standards and requiring states to enact specific legislation within two legislative sessions? (The alternative

is for these protections be embodied in Federal law and required of states as a condition of receiving Federal funds.)

Option 1: General Federal standards; specific state action:

There is general agreement that privacy protections should be basically uniform. However, considerable disagreement exists as to how such uniformity should be achieved.

The Commission argued that each state should be able to decide its specific requirements within the context of general Federal standards. In the past, Federal agencies have not exercised strong oversight of state record-keeping practices, even where the requirements were clear. Some Federal agencies lack the resources to monitor state practices adequately. It is also believed that state laws would be more effective because the states could shape the requirements to fit local conditions and would have a greater stake in enforcing their own laws. Also, only state laws could cover programs not receiving Federal funds.

Option 2: Specific Federal standards as condition of funding:

DHEW opposes the Commission's proposal. First, the proposal marks a departure from the Federal government's traditional approach of ensuring the protection of individuals by the states, as with the civil rights laws. Second, the Commission's approach is thought to be cumbersome and possibly productive of divergent practices from state to state. Third, the Commission's proposal ignores the Federal government's responsibility to itself ensure the proper expenditures of Federal funds.

Decision:

_____ Adopt the Commission proposal of general Federal standards and required specific state legislation.

_____ Adopt the DHEW proposal of specific Federal requirements being a condition of receiving Federal funds.

3. Should Federal law require states to provide by statute that public assistance and social service agencies must have reasonable procedures to ensure the accuracy, timeliness, completeness, and relevance of the records they maintain and disclose?

For a general discussion of this issue see "Propriety and Relevance of Information Collected" in Section I.G.2 and "Accuracy, Timeliness, and Completeness" in Section I.G.6. above.

Pro:

This is the Commission recommendation, and is supported by the Department of Labor. The Commission believed that public assistance and social service agencies, unlike private sector record keepers, do not have an obvious interest in assuring the accuracy, timeliness, completeness, and relevance of their records, and currently are not required to do so by Federal law. Such a requirement would encourage these record keepers, for example, to reinvestigate third-party source information before relying on it to make a judgement, and might prompt agencies to ask the client to explain document information that may be inaccurate before incorporating it in the file. The Commission believed that such an incentive is appropriate given the subjective nature of the information collected and maintained by these agencies, and the fact that not all personnel employed by these agencies have adequate professional training to properly evaluate its usefulness. Finally, because these are public agencies, such a requirement would not involve costly regulation and litigation, as it might in the private sector.

Finally, the Commission recommended that social service and public assistance agencies adopt reasonable procedures to ensure relevance, as well as accuracy, timeliness, and completeness. It did so here and not in the private sector areas because it believed that, as government agencies, these record keepers should be subject to the same requirements as the Federal government which, under the Privacy Act, may maintain only information which is "relevant and necessary" to accomplish a purpose of the agency. The Commission did not believe that this would entail unnecessary regulation by the Federal government.

Con:

The Department of Health, Education, and Welfare strongly supports the objective of the Commission's recommendation, but believes it inappropriate for the Federal government to legislate on the subject. Several agencies also suggest that there is no demonstrated need to mandate these procedures by statute, and that it might be intrusive for the Federal government to require such procedures of State institutions. There is also a concern that such a statute would be impossible for the Federal government to enforce.

Decision:

_____ Yes, Federal law should require states to provide by statute that public assistance and social service agencies must have reasonable procedures to ensure the accuracy, timeliness, completeness, and relevance of the records they maintain and disclose.

_____ No.

J. Telephone Toll Records

Description of Records

Telephone conversations between private persons are confidential, absent the consent of one party for a third party to overhear or monitor the conversation. Under present law, severe restrictions control the monitoring of such communications. If improperly gathered, the records of unauthorized telephone monitoring will be excluded as evidence in a court of law and could become the basis for a criminal action against the collector.

There is, however, a bi-product of telephone communications which may reveal significant information about an individual and for which no such restrictions apply. This bi-product is the telephone toll record--the record indexed by the name or number of the individual listing all toll calls (local or long distance) made by him and the telephone number to which he spoke. The Commission recommended that there be an expectation of confidentiality for these records.

Current Law and Practice

The American Telephone and Telegraph Company, which maintains most of the telephone toll records created in the United States, now refuses to disclose toll records unless presented with a subpoena or other legal order. However, when presented with a subpoena or legal order compelling disclosure, a telephone company is currently under no legal requirement to notify the individual prior to releasing the records, or even to indicate afterwards that this has occurred. Moreover, subpoenas will often be issued in ex parte proceedings, and the individual has no legal interest to assert against the government's claimed need for access to this information about him.

Issue for Decision

1. Should the individual have an expectation of confidentiality (as defined in Section I.G.7) for telephone toll records?

Pro:

The Commission recommended that there be an expectation of confidentiality for these records because it

believed that the mere fact of communication between two parties may be as revealing as the content of the communication. While, in practice, these records are not made available to outside parties without a subpoena or legal order, the Commission's position was that the individual currently is not afforded adequate protection when such a legal request is made. Without the full provisions of the expectation of confidentiality, the individual is not given prior notice of the request and standing and legal interest to challenge the disclosure in a court of law. Finally, government is already required to obtain a search warrant in order to monitor telephone conversations and obtain the content of such communications, and the Commission saw no compelling reason not to extend this requirement to the record of whom the conversation was between.

Con:

The primary objections to this proposal come from the law enforcement community, which argues that access to these records is necessary to accomplish its mission. It is argued, moreover, that they are of particular value in combatting organized crime. To require prior notification to the individual before releasing the records to the government would be burdensome and, perhaps, compromise these investigations.

Decision:

_____ Yes, an expectation of confidentiality should be created for telephone toll records.

_____ No, an expectation of confidentiality should not be created for telephone toll records.

## III. Government Access to Personal Records Held by Third Parties

### Issues

Part II of this memorandum presented decisions concerning the expectation of confidentiality that an individual may have in connection with records maintained by certain private sector record keepers (e.g., credit grantors, banks, medical care providers, insurance institutions, and employers), and in telephone toll records. The primary issues presented in this section are: (1) what should be the scope and nature of the process used by government to obtain records where it has been decided that an individual should have a legally enforceable expectation of confidentiality; and, (2) where an individual does not have such an expectation, to what extent should there be procedural requirements on government collection of records from other governmental record keepers and from private sector institutions.

Government has unique powers to collect and use information, powers which are ordinarily used quite legitimately, but which can also be employed to coerce individuals. As a result, our legal system has traditionally incorporated safeguards to balance the powers of the state with necessary protections for the individual. As discussed in the introduction, however, concern over the effectiveness of the traditional safeguards has emerged because of an important, though gradual, change in record-keeping patterns. Today, sensitive personal information that historically would have been held in the individual's exclusive custody is maintained by third-party record keepers, such as credit-card issuers or banks, who require this information in order to provide vital services. This change in record-keeping patterns has outflanked traditional legal protections, such as the Fourth Amendment to the Constitution, and permits government agencies to collect personal information through informal, unrecorded requests that leave the individual without knowledge of, or control over, the access process.

### Current Law and Practice

At present, a private sector record keeper, such as a bank or credit-card issuer, may comply with a government request for access to personal information as it pleases, without regard for the wishes or expectations of confidentiality of the individual to whom the record pertains. Most third-party record keepers generally

comply voluntarily with government requests. In addition, this process of informal access is the usual means by which government investigators collect the information they need. This is not the case, though, in California where private sector record keepers operate under a state constitutional requirement that creates what amounts to an expectation of confidentiality in personal information held by certain third parties.

For the rest of the nation, however, prevailing law is most clearly expressed in the Supreme Court's decision in United States v. Miller, 425 U.S. 435 (1976). In that decision, the Court explicitly stated that customer account records in a bank are not the private papers of the customer and that the individual has no legal interest in protecting the confidentiality of those records, including no ability to raise Fourth and Fifth Amendment objections when the government seeks access to the records. The Court reasoned that an individual has neither ownership nor possession of such records; the records are simply the "business records of the bank."

The crucial element in this legal formulation is that an individual, lacking a "proprietary interest" in a bank's records of his account, is without a legal basis upon which to challenge government access to those records. Credit, insurance, medical, and telephone toll records are similarly not subject to an individual's control. In other words, current law does not establish a duty of confidentiality on the third-party record keeper. Without creation of such a duty, even if the record keeper notified the individual and the individual had standing in court to challenge the government's action, the only interest that he could raise would concern at most technical and procedural challenge rights and thus would provide little effective protection.

Finally, in addition to using informal modes of access and the constitutionally delimited process of the search warrant, the Federal government obtains records and written information through the use of three basic forms of compulsory legal process: administrative summons, grand jury subpoena, and judicial subpoena in the course of litigation. A subpoena or summons is simply a form which a government agency or attorney fills in to show who is commanded to appear, with what document or testimony, and when and where he should appear. An agency must have explicit legislative authority to issue an administrative summons and the form is

prepared by an official of the agency involved. For a judicial or grand jury subpoena, the blank form is obtained from the clerk of a district court and is subject to court supervision if challenged by the record holder.

Agency Participation

One of the task groups created as part of this review process specifically addressed the Commission's government access recommendations. The agencies represented were: Department of Justice, Department of the Treasury, Department of Defense, Department of Health, Education and Welfare, Department of Labor, Central Intelligence Agency, Federal Reserve System, Civil Service Commission, Veterans Administration, General Services Administration, Federal Communications Commission, and Federal Home Loan Bank Board.

The scope of responses received from these agencies ranged from complete rejection of the Privacy Commission's recommendations to limited acceptance of them. No agency fully accepted all of the recommendations. The Justice Department, as the result of the work of an internal task group, developed a detailed alternative proposal which adopted the fundamental principles presented by the Privacy Commission, while attempting to reduce some of the difficulties which it believed the Commission's specific recommendations would create for law enforcement and other government functions. The Department of the Treasury has joined in the Justice position, and this alternative has been presented by the two Departments to the Congressional committees legislating in this area. References to the particular positions of the Justice and Treasury Departments below are to their position as presented to the House Banking Committee in preparation for its mark-up of H.R. 13088 on July 11, 1978. The Committee has since reported out a bill incorporating the Justice proposal with some modifications. References to agency positions (other than the positions of the Departments of Justice and the Treasury) are to positions expressed in the Report of the "Privacy Study Task Groups #2," March 21, 1978.

This memorandum, and the agency task group review that led to it, focuses on records maintained by several types of private sector record keepers and by state and local governments. The Departments of Justice and the Treasury have presented a detailed position

on government access policy which, however, is limited to bank records. For the purpose of this discussion the positions of Justice and the Treasury, to the extent applicable, are treated as if they applied to all records discussed. In addition, some independent regulatory agencies, such as the Securities and Exchange Commission, object to the application of any of these requirements to them and are seeking total legislative exemptions.

This process has identified areas of agreement as well as disagreement among agency positions. This section first sketches the areas of agreement and then presents those areas of important disagreement where decisions are necessary.

Areas of Agreement

There is general agreement throughout government that new legal protections for personal privacy need to be established when government seeks records about individuals held by certain private sector record keepers. Specific agreement exists as follows about what some of the elements of such protection should be.

1. Notice to an Individual of Government Access to His Records

The Privacy Commission and the executive agencies, including the Departments of Justice and the Treasury, agree that certain private sector record keepers should not be permitted to disclose personal information to the government except through some form of legal process, though the executive agencies feel that the process need not be compulsory (see issue 1 below). All parties agree that the interests of the individual citizen should be balanced against government's need for the information before disclosure; ordinarily, records could be disclosed only if the subject were given notice of a government access request and an opportunity to challenge the potential disclosure in court. Presumably, the records to be covered by this requirement would be all those in which an expectation of confidentiality has been adopted in Part II, but there has been no specific agreement so far on records other than bank records.

There is also agreement among the agencies that some exceptions to the notice requirement should be made (though disagreement exists over what the specific

exceptions should be). All parties are agreed that implementation of these recommendations, to whatever degree, would require reform of the existing notice and challenge procedures relating to the use of compulsory process.

2. Protections Would Only Apply When the Individual to Whom the Records Pertain is the Subject of an Investigation

The Commission and the agencies agree that the proposed governmental access recommendations should apply only if the personal information being sought pertains to an individual who is the subject of, or likely to become publicly implicated in, the investigation for which the access request was being made. The recommendations would not apply if the record keeper is the subject of an investigation in which individual records are needed to prove the case against the record keeper. Consequently, many requests for access to personal information made to private sector record keepers by supervisory and regulatory agencies, and some requests by law enforcement agencies, would not be covered by the proposed access limitations. Thus, the provisions would not apply if an agency sought all of the records of a company to determine if the company, and not individual customers, had violated the law.

The Justice/Treasury proposal offers two further safeguards to protect the interests of individuals whose records are sought for such a purpose. First, the agency would be required to give the record keeper a sworn statement attesting to compliance with the provisions of the government access statute. Second, when personal records were obtained pursuant to such a sworn statement, the records could not be transferred to other government agencies for prosecution or used against an individual; the second agency could be notified that a violation might exist but could only obtain the records by giving the individual notice and an opportunity to contest the second agency's access.

3. Protections Only for Natural Persons

Because of the terms of its mandate, the Privacy Commission's recommendations apply only to natural persons. Partnerships, corporations, and other business entities, even if composed of only one or two individuals, are not covered. The limitations of the Commission's mandate notwithstanding, the executive agencies agree that

the recommendations should apply only to natural persons. (Some disagreement with this position has been expressed in Congress, some Members believing that an individual should not be deemed to have given up his rights simply because of his participation in a business entity.)

4. Exclusion of Search Warrants

The Privacy Commission excluded search warrants from its proposed access limitations. The Commission observed that search warrants can be obtained only after an ex parte hearing at which evidence is presented to a neutral magistrate sufficient to meet the Fourth Amendment's "probable cause" requirements. In addition, search warrants are most frequently used to collect information directly from an individual and do not ordinarily involve the record-keeping relationship issues which this memorandum addresses. However, the Commission urged that further study be given to the question of what papers may be seized with a search warrant.

This call for action was recently echoed by the press and some Members of the Congress in the wake of the Supreme Court's decision in Zurcher v. Stanford Daily (46 U.S.L.W. 4546, May 31, 1978), which upheld the use of a search warrant to seize evidence held by a newspaper which was not itself accused of any crime. In light of Zurcher, the Administration is evaluating the desirability of strengthening the protections on the use of search warrants. This issue is not being treated as part of this review process.

Areas of Disagreement

The disagreements between the Privacy Commission and the agencies primarily center around: (1) the nature of the proposed protections where an individual is deemed to have an expectation of confidentiality; and (2) the application of certain of the recommendations to all types of records and to state and local government record keepers. This set of issues for decision involves situations in which government seeks records in the course of a particular investigation or administrative proceeding. The section will also present an issue for decision that relates to statutes requiring private sector record keepers to report personal information automatically and routinely to government authorities.

A. Nature and Substance of Protections Where an Individual is Deemed to Have an Expectation of Confidentiality

This group of issues defines the process that will be used for access to the records in which individuals are to be given an expectation of confidentiality. This expectation of confidentiality has been defined in Section I.G.7, and the kinds of records to which it applies have been identified in Part II.

1. Should government access to confidential records always be through compulsory process?

The Commission recommended that government access to personal information in which there is an expectation of confidentiality be permitted only through use of compulsory process. The Departments of Justice and Treasury recommend that, at least for bank records, the agencies or their components that do not have legal authority to use compulsory process be authorized by law to obtain records by using a "formal written request" procedure which they have developed.

The Justice/Treasury formal written request proposal would create a new form of process, though not a compulsory one. This process would provide notice to the individual and standing to contest the government's request in court. If the individual failed to make a challenge within the required time period, or if a court rejected his challenge, the record keeper would be free to exercise its own judgment concerning compliance and would have immunity from civil liability to the customer if it released the requested records to the government. However, unlike the compulsory process proposed by the Commission, the record keeper would not be required to make disclosure in response to a "formal written request." The precise form of a "formal written request" could be established by regulation by each agency involved, and need not be specifically authorized by the Congress, which would set forth only the general framework of the request procedures.

Option 1: Compulsory process

Three arguments support the Commission's proposal for exclusive reliance upon compulsory process to obtain confidential personal records. First, many banks currently require the government to use compulsory process and the Commission was

not persuaded that this unduly restricts law enforcement investigations. Second, although the Justice/Treasury proposal gives record keepers discretion to refuse disclosure, even when the individual does not exercise his privacy rights, the practical effect may still be that formal written requests will be seen as compelling disclosure, especially in view of the disclosure pressures reportedly perceived by most private sector record keepers.

Finally, although the proposed formal written request procedure includes protections for the individual that are now missing when agencies make requests for records, the proposal involves a Congressional endorsement of a formal access procedure available to all agencies. This runs counter to the traditional notion of careful and limited grants of police power and may have the effect of increasing government collection activities. Assuming that most record keepers would comply with these formal written requests, the effect--especially when exceptions to the notice requirement are made--may be to give every Federal agency the equivalent of compulsory process powers.

Option 2: Formal Written Request:

Three arguments support adoption of the Justice/Treasury formal written request scheme. First, most investigative agencies currently rely on informal modes of access to obtain the records needed to carry out their investigative functions. It is unclear whether other agencies with criminal and civil investigative jurisdiction will be able to effectively carry out their functions, because they do not have adequate access to compulsory process. Legislating administrative summons powers for all these agencies will be a slow and uncertain process. The use of formal written requests will allow them to continue obtaining information, while at the same time protecting individual privacy.

Second, the formal written request proposal accommodates privacy considerations by incorporating rights of notice and challenge. This is a far greater protection than is currently required by law.

Third, the Department of Justice has asserted that reliance on existing forms of compulsory process will unduly restrict law enforcement

investigations. If the formal written request scheme is not accepted some segments of the department will be forced to rely exclusively on, and thus burden, the grand jury process to obtain records.

Decision:

_____ Require the use of compulsory process for all government access requests for those types of records in which the individual has an expectation of confidentiality.

_____ Permit agencies or their components that do not have authority to issue subpoenas or administrative summons to use a formal written request procedure for those types of records in which the individual has an expectation of confidentiality.

Collateral Decision:

Staff note: Regardless of the option selected above, the collateral question is raised of seeking legislative authority for administrative summons powers for agencies or components thereof that do not now have access to compulsory process but need to acquire personal records for which there is an expectation of confidentiality. While some agencies have informally expressed an interest in this regard, there is presently insufficient data to enumerate the strengths and weaknesses of this option.

_____ Seek legislative authority for administrative summons powers for _____.

2. What should be the nature of the judicial standard which can be employed by an individual in order to make the government justify its access request?

As discussed earlier, the Commission and the Justice and Treasury Departments agree that a Federal law should be enacted to give an individual the two elements of a protectible legal interest in records held by private sector record keepers in which he has an expectation of confidentiality. First, the individual would have the right to be notified of a government access request and the opportunity to go to court to challenge the request and protect his interests. Second, the substance

of the legal interest which the individual was seeking to protect in any challenge would be defined in a legislative standard. Such a standard is the heart of the protectible legal interest, vital in giving effect to any protection for a citizen's records. Notice of a government request to obtain an individual's records and a right to challenge that request are of little value without a defined legal interest which can be used to test the legitimacy of a government inquiry, requiring government to justify its request. Basic disagreement exists, however, between the Privacy Commission recommendation and the Justice/Treasury proposal over the specific nature of the challenge rights and the definition of the legal standard.

The Commission recommended that an individual challenging a government request for records in which he had an expectation of confidentiality be provided with a legal interest which includes both the right: (1) to require from the government evidence of the "reasonable relationship of the record sought to the investigation underway"; and (2) to assert the protections which he would have under the Fourth and Fifth Amendments if the records were in his possession. The Commission believed that this second part of the interest did not rise to the level of forcing government to meet the "probable cause" standard required to obtain a search warrant; rather, as a result of recent Supreme Court opinions, the Commission concluded it could best be characterized as a "reasonable cause" standard which government would have to meet in order to justify access to an individual's records.

The Justice/Treasury proposal would require an individual whose records are sought to file a motion and affidavit in an appropriate Federal district court: (1) stating that records pertaining to him have been sought; and (2) "showing a factual basis for concluding that there is no reason to believe that the records sought contain information relevant to a legitimate law enforcement purpose." The agency would then have to establish to the satisfaction of the court that the documents requested were relevant to a "legitimate law enforcement purpose" -- which includes administration or enforcement of any civil or criminal statute, rule, or regulation within the authority of the agency making the request.

The two proposals differ on the following three points: (1) the Justice/Treasury proposal would place on an individual challenging an access request the burden of coming forward with facts to suggest why government's request is unjustified, rather than requiring, as does

the Commission's proposal, that the government present evidence justifying a request in the first instance; (2) it is unclear whether the Justice/Treasury proposal would require the government to establish the relationship of the request to a specific investigation, a requirement of the Commission proposal; and (3) the Justice/Treasury formulation offers a less burdensome substantive standard for government agencies to meet in order to justify access than does the Commission proposal.

Option 1: Commission Position:

The Commission concluded that only by requiring government to take the initial burden of justifying its request before any showing by the individual, and by adopting a relatively high standard against which to test the adequacy of government's justification, could government agencies be prevented from seeking more information than they need, or from seeking information without sufficient grounds. By forcing attention in each case to questions of relevance, propriety, and a specific and justifiable government interest, an individual's legitimate interests in his bank and similar records can be most effectively recognized, and the potential for improper actions by government checked.

The Commission's proposal would require the government to carry the burden of showing that the records sought are relevant to a legitimate and specific investigation. The Justice/Treasury proposal places the final burden of making this justification on the government, but requires the individual to first produce facts demonstrating that there is no reason to believe that his records are relevant to a legitimate law enforcement purpose. The individual, as a result, is put in the position of demonstrating what is, or is not, a legitimate law enforcement purpose, rather than merely being required to make a non-specific objection which triggers a government duty to file. This could make it almost impossible for an individual to effectively initiate and sustain a challenge.

Finally, the relatively high substantive standard recommended by the Commission as part of an individual's protectible legal interest assures that a good deal more than mere suspicion will be needed to justify government access to a citizen's private records.

Option 2: Justice/Treasury Position:

The Commission's proposal may cause undesirable adjudicatory delay by allowing procedural objections to be raised. The requirement that an individual have the burden of coming forward to show why there is no relevant law enforcement purpose for the records to be disclosed is necessary to discourage frivolous challenges and dilatory tactics. If an individual did not have such a burden he might force the government to waste considerable time, expense, and effort even though there was no legitimate basis for his challenge. Experience under the Tax Reform Act of 1976 indicates that frivolous challenges can be a problem.

The Commission's substantive standard is so high that government agencies may not be able to meet their burden, particularly at the early stages of an investigation. In particular, the imposition of such standards may jeopardize the prosecution of white collar crimes, where financial record information is crucial at the early stages of investigation. There is some experience in California, where the applicable standard is similar to the standard proposed by the Commission (though somewhat higher), which indicates that delays and premature termination of investigations may result.

Finally, the procedures and substantive standard in the Justice/Treasury proposal are a significant step forward from the present legal situation where an individual has no rights. Moreover, the substantive standard will cause the process to be subject to individual and public scrutiny, as well as court supervision, which will act as a significant check on any abuses.

Option 3: Compromise Position:

A compromise option would be to establish a substantive standard for disclosure between that recommended by the Commission and that contained in the Justice/Treasury proposal. It would require the government to show a reasonable relationship between the record requested and an ongoing investigation of a violation of law, but would not adopt the Commission's substantive standard by giving the individual the equivalent of Fourth and Fifth Amendment protections for the records requested.

This option would, however, adopt the Commission's approach of placing the initial burden on the government by dispensing with the Justice/Treasury requirement that the individual first come forward with a showing that the government's request is unjustified.

This formulation has the effect of placing the principal burden on government to make an initial showing of legitimacy by establishing the connection between the records sought and a specific investigation of a violation of law. In so doing, the approach offers protection against use of process for "fishing expeditions." At the same time, elimination of the requirement that the government overcome the equivalent of an individual's "Fourth and Fifth Amendment" interests will ease the danger of excessive impairment of government investigations. On the other hand, it offers limited protection against challenges made only to delay or impair legitimate investigation.

Decision:

_____ Adopt Commission proposal: burden on the government to establish specific relevance of its request first; "reasonable cause" standard.

_____ Adopt Justice/Treasury proposal: burden on individual to come forward and establish factual basis for questioning propriety of government request; "legitimate law enforcement purpose" standard.

_____ Adopt compromise: burden on government of initially coming forward; "reasonable relationship of record sought to an ongoing investigation of a violation of law" as sole standard.

3. What should be the exceptions to the notice and challenge rights?

The agencies and the Commission agree in general that when a government access request for personal information for which there is an expectation of confidentiality is directed at a third-party record keeper: (1) the individual to whom the record pertains should receive a copy of the request from the requesting agency at the same time that the request is served upon the

record keeper; and (2) that the individual should have an opportunity to go to court to challenge the request. To the extent that there is disagreement, it centers around whether there should be exceptions to these notice and challenge rights.

The Commission's proposal would never permit an agency to dispense with notice prior to obtaining records, if the personal information being sought were one of the categories of personal information considered confidential (i.e., for which the record keeper was under a duty of confidentiality). The government, of course, always has the option of obtaining a search warrant, which avoids the prior notice to the individual.

The Justice/Treasury proposal recognizes an individual's expectation of confidentiality but also enumerates certain conditions in which privacy interests would yield to other important societal interests. Agencies could obtain a court order for a delay of a notice if there were reason to believe that prior notice would result in endangering the life or safety of any person, flight from prosecution, destruction of or tampering with the evidence, intimidation of potential witnesses, or would otherwise "seriously jeopardize" or "unduly delay" the investigation. In addition, an agency could have access to records without giving the individual prior notice and without first obtaining a court order delaying or dispensing with notice in the following circumstances:

(1) if a grand jury subpoena were used. (This topic will be treated below as issue 6.)

(2) if the investigation involved either foreign counter or positive intelligence activities; or protection of the President. (However, the agency must give the record-keeping institution a sworn statement that the access complies with the provisions of the government access statute).

(3) if an emergency situation existed in which there were an imminent danger of flight, destruction of records, or a threat to life or safety. (However, the emergency exceptions would be subject to a requirement that the agency provide: (a) a written representation of an emergency to the record keeper; (b) an affidavit to a court within five days

after access justifying the use of the emergency procedures; and (c) the individual with notice of the access at the expiration of a court ordered period of delay or, in the absence of such an order, as soon as practicable.)

Option 1: No exceptions:

The Commission's approach is more likely to safeguard an individual's privacy because it far more strictly restricts access to confidential personal information. If the government could actually make a showing in court which would sustain an exception to the prior notice and challenge requirements, then the government is likely to have the requisite probable cause to obtain a search warrant.

In addition, the Justice/Treasury formulation contains a relatively broad definition of the circumstances that would permit a court to issue an order delaying notice to the subject. Since the conditions for waiver are broadly drawn, courts may tend to routinely grant applications for waiver of notice. This is particularly likely where exception can be made if prior notice "otherwise jeopardizes an investigation."

Finally, the Justice/Treasury formulation, in some circumstances, permits agencies to dispense with notice without the check of prior court supervision. The argument that court supervision is impractical and inappropriate for foreign intelligence, Presidential protection, and emergency investigations is compelling if the scope of what is considered foreign intelligence or Presidential protection services is tightly interpreted. This is uncertain without the protection of court supervision.

Option 2: Some exceptions:

The principal deficiency in the Commission's approach is that it is unyielding in the requirement that notice be provided prior to access to the categories of information for which there is an expectation of confidentiality. Under the Commission's approach, it would not be possible in many instances for a government agency to obtain credit, banking, medical, or insurance records (assuming the duty of confidentiality has been elected in Part II) without first giving the individual notice and

an opportunity to go to court. The only exception, of course, would be where the government uses a search warrant, with its relatively high standard of probable cause -- a standard far higher than that which would be needed to sustain the proposed exceptions.

The Justice/Treasury proposal, except in a few circumstances, assures either prior court review or individual notice before agencies can obtain access to personal information for which there is an expectation of confidentiality. It is argued that the position of no court supervision is justified for foreign intelligence activity because the current definitions of foreign intelligence activity are accepted by Congress and to require disclosure of such activities to a court may seriously jeopardize those activities. The same is true of investigations in connection with protecting the President. As an additional protection, where such access occurs without court supervision the agencies will be subject to review by the appropriate Congressional oversight committees. The only other area where there is no prior court review is in certain life-threatening emergency situations in which it is reasonable to dispense with prior notice in order to prevent harm from occurring. Even there, however, the agency must file a justification for the access in court within five days.

Option 3: Compromise:

There is a possible compromise between these two positions which adopts the Justice/Treasury formulation, except that it would tighten the grounds upon which a court could delay notice to the record subject. (No notice would be provided, within the standards suggested by Justice/Treasury, in foreign intelligence and Presidential protection situations.) A judge could waive notice only where the government presents facts to establish: (a) that the substantive standards for using a subpoena as described in issue 2 above are satisfied; and (b) that notice would be likely to result in: (i) endangering the life or safety of any person; (ii) flight from prosecution; (iii) destruction of, or tampering with, evidence; or (iv) intimidation of potential witnesses.

Permitting waiver of notice because it would "otherwise seriously jeopardize the investigation," a standard

included in the Justice/Treasury proposal, would not be included because it allows too much flexibility. The limitations listed above encompass the specific circumstances which might jeopardize an investigation, and waivers should be limited to such circumstances. This compromise would provide the basis for meaningful court supervision and balances the interests presented by the Justice and Treasury Departments and the Privacy Commission, without running the danger of overly broad formulations which might be misused.

Decision:

_____ Adopt the Commission notice and challenge proposal.

_____ Adopt the Justice/Treasury notice and challenge proposal.

_____ Adopt the compromise set forth above.

4. Should judicial subpoena in the course of litigation be covered?

The Commission recommended that government use compulsory process for access to personal information in which an individual has an expectation of confidentiality, when that individual is already involved in a judicial proceeding with the government (both civil and criminal). The individual would have rights of prior notice and challenge and recognition of the substantive legal interest decided above.

Pro:

Under the procedures that today govern civil and criminal litigation, a litigant has a right of notice when the government seeks access, and a right to challenge that access on the grounds that the documents sought are not relevant to the case being tried. The Commission proposal would increase the grounds on which the individual could challenge access by bringing into play a new substantive legal interest--the "expectation of confidentiality" decided in Part II of this memorandum. Absent this provision, the result would be looser controls over government access to documents in the course of litigation than at other times, which is just the opposite of the situation today.

Con:

The Federal Rules of Civil Procedure and Criminal Procedure contain detailed, well worked-out, and sufficient protections for documents sought by the government in connection with litigation to which the government authority and the individual to whom the documents pertain are parties. The individual receives notice and an opportunity to litigate issues of relevance. It will be confusing and burdensome to courts and litigants to create special procedures applicable only to those records in which the litigant has an "expectation of confidentiality."

Decision:

_____ Apply the access proposals to judicial subpoena in the course of litigation.

_____ Exempt judicial subpoena from access proposals in the course of litigation.

5. Should the standards for the issuance of, and use of information obtained by, administrative summons be reformed?

The Commission recommended tightening the procedures for the issuance of administrative summons and imposing limitations on the use of personal information obtained by administrative summons. Specifically, the Commission recommended that Federal law provide that:

a) an administrative summons may be used only to inspect records required by law to be maintained by the record keeper;

b) the information acquired with the administrative summons may be used only for purposes of the investigation or enforcement action which justified acquisition of the information; and

c) an administrative summons must be issued by a supervisory official and not a field agent.

Pro:

The Commission argued that use of administrative summons by a wide variety of Federal agencies is expanding without adequate control and restrictions. Specifically, there is little supervisory control of when and for what purposes a summons is issued. The Commission developed evidence that administrative summons are frequently issued by field agents rather than supervisors. In addition, the Watergate and Intelligence Committee investigations identified questionable or improper uses of administrative summons power.

Limitations on issuance procedures and on the permissible uses of information obtained from administrative summons are necessary to limit intra- and interagency sharing of personal information, and the use of the information for a purpose unrelated to the purpose of the original investigation. The Commission concluded that the strictures found in current law, including the Privacy Act, are ineffectual in controlling the exchange of personal information within the government, particularly for law enforcement purposes.

Con:

Counterarguments are directed primarily to that portion of the Commission's proposal that places limitations on government use and retention of this information, not on the limitations on access. It is argued that the Privacy Act should control information use without being subjected to piecemeal exception.

If administrative summons procedures are to be reformed, this should be done on a comprehensive basis, not just in the context of access to records. This sort of sweeping reform requires a broader study than the Commission undertook. The Departments of Justice and the Treasury have not spoken in detail to this proposal.

Decision:

_____ Adopt Commission issuance and use recommendations.

_____ Retain present law without change.

6. Should the standards protecting the secrecy of information obtained by a grand jury which assure protections for individuals under investigation be reformed?

The Commission's proposed grand jury reforms would require that personal information obtained through use of a grand jury subpoena:

a) be returned and actually presented to the grand jury;

b) be employed only for a criminal prosecution where the grand jury issuing the subpoena issued a presentment or indictment;

c) be destroyed or returned to the record keeper where no indictment or presentment is issued (except to the extent that the information has become part of the official minutes of the grand jury);

d) not be copied or kept apart from the sealed records of the grand jury; and

e) be protected by stringent penalties for improper use or disclosure outside the grand jury.

Pro:

In support of its grand jury reforms, the Commission observed that use of the grand jury subpoena suffers from a significant discontinuity between theory and practice. The use of a grand jury in criminal prosecutions is constitutionally mandated and shrouded, in theory, with certain protections. The grand jury subpoena permits the grand jury to collect virtually any evidence it desires. To balance this power, the deliberations of a grand jury, and the testimony and other information it obtains, are theoretically protected by a strict standard of secrecy. But, the Privacy Commission found that, in practice, the grand jury subpoena has to a significant extent become an administrative tool in assisting prosecutors to collect information. Its current use is characterized as a device employed by investigators to circumvent the more stringent requirements which must be met to obtain a search warrant. According to the Commission, documents are often subpoenaed by government investigative

agents without the knowledge or the approval of the grand jury. The Commission found that information obtained by investigators using grand jury subpoenas may never reach an attorney for the government, let alone the grand jury; it may simply be retained in the files of the investigative agency for unspecified future use.

The Commission also argued that Rule 6(e) of the Federal Rules of Criminal Procedure, which currently governs the information collection practices of Federal grand juries, is insufficient protection because it contains many ambiguities. Rule 6(e) requires the prosecutor to obtain a court order as a precondition to disclosing "matters occurring before the grand jury," and limits that disclosure to one "preliminary to or in connection with a judicial proceeding." There is no definition of "matters occurring before the grand jury" and it is not clear that this formulation covers records subpoenaed but not returned and presented to the grand jury. The rule does not provide for notice or standing to the individual if the prosecutor applies for a disclosure order. Rule 6(e) permits disclosures to investigators assigned to the investigation, but does not restrict subsequent disclosures of summaries or abstracts of subpoenaed documents (one of the problems identified by the Privacy Commission), since the summaries and abstracts are not "matters occurring before the grand jury." What case law exists suggest that the traditional safeguards for information obtained for the grand jury, as reflected in Rule 6(e), have been rendered ineffectual and that the problems identified by the Commission remain unremedied.

Con:

The Departments of Justice and the Treasury urge that the grand jury subpoena process be exempt from the access limitation proposals. They take the position that the Federal Rules of Criminal Procedure should control grand jury information use without being subjected to new and piecemeal limitations. The Departments of Justice and Treasury point out that Rule 6(e) currently limits the prosecutor's right to disclose information obtained in a grand jury investigation. They believe that the rule's requirement of a court order before the prosecutor can disclose grand jury matters,

and limiting that disclosure to a use "preliminary to or in connection with a grand jury proceeding," already provides adequate protections. Furthermore, it is illogical to subject only one type of records obtained from a limited number of sources (records in which an individual has an expectation of confidentiality) to special restrictions on use.

Decision:

_____ Adopt Commission grand jury recommendations.

_____ Adopt Justice/Treasury approach and retain present law without change.

B. Extension of parts of government access recommendations to records where an individual does not have an expectation of confidentiality and to the collection practices of state and local governments.

The Commission and the Departments of Justice and the Treasury agree that for private sector records the provisions for full individual notice and challenge rights (as just decided) should apply only where it has been determined that an individual has an expectation of confidentiality in connection with certain record-keeping relationships as discussed in Part II of this memorandum. The areas of disagreement concern whether the scope of these provisions should be extended in whole or in part to other record-keeping situations.

7.A Should government requests for private sector records other than those covered by an expectation of confidentiality (as decided in Part II) be documented by a "paper trail" to create greater accountability?

The Commission recommended that government access to personal information from private sector record keepers in which the individual does not have an expectation of confidentiality require the use of legal process. In many instances (grand jury subpoenas constitute the major exception), the Commission's proposal would mean that the individual receive notice of the access request and an opportunity to raise at least procedural objections in court. This approach has been rejected by everyone within government.

Many executive agencies do, however, urge that where Federal agency access is obtained without individual

consent to non-confidential records, the agencies should be required to make the request on an agency letterhead to the record keeper. "Letterhead" requests would not require notice to the subject or an opportunity for a court challenge and, as a legal matter, would not compel compliance by the record keeper. (This issue was not addressed by the Departments of Justice and the Treasury in their testimony on access to financial records because that testimony concerned only bank records for which there would be an expectation of confidentiality.)

Option 1: Letterhead Request

The Commission and most agencies believe that because much of the information collection by the government is done in an informal manner, neither the individual nor anyone else may ever know that a request to, and consequest disclosure by, a private sector record keeper has been made. The government should therefore be required to leave a paper trail of its investigation. This can be accomplished by requiring an agency to make all requests for information in writing, on an agency letterhead.

To require the additional step of legal process, as the Commission suggested, adds considerably to an agency's administrative burden, and adds nothing to the interests of creating a paper trail that will not be satisfied by a letterhead request. Legal process is only necessary if notice and challenge rights are important, which is not the case for these non-confidential records. Requiring a letterhead request would cause a "paper trail" to exist in two places: (1) the government agency making the request; and (2) the organization releasing the information. Consequently there is an opportunity for government and individual oversight. Documentation of government information collection activities will be valuable for investigating and assessing the legitimacy of government investigative conduct and the disclosure practices of private sector organizations. This is the position of all of the responding agencies.

Option 2: Compulsory Process

The Commission supported the need for a paper trail for the reasons set forth above, but did

not examine letterhead requests. It can be argued that, because a letterhead request does not provide notice to the individual, it is less likely to result in questionable government collection activities coming under public scrutiny. Since an agency's compulsory process powers have received specific congressional approval or review through a judicially controlled and supervised process, compulsory process provides greater protections than a letterhead request.

Option 3: No Paper Trail (status quo)

It is inappropriate to require the government to use a letterhead request to obtain information which, by definition, the individual does not expect will be treated in a confidential manner.

Decision:

_____ Letterhead request

_____ Compulsory process

__✓__ No paper trail

7.B Should requests by Federal agencies for personal records held by state and local governments be subject to some restrictions?

The Commission recommended that some form of compulsory legal process be used whenever the government seeks personal information for purposes of making a decision about an individual from any private sector record keeper and any agency of another governmental jurisdiction. The Departments of Justice and the Treasury have not spoken to this issue; however, the Department of Defense has expressed its opposition to a formal process requirement.

Option 1: Letter Head Request

The letterhead approach rests on the desirability of creating a uniform system of government collection. Since there is a great deal of sensitive personal information that flows from state governments to the Federal government, there is need to have a record that will establish what information was exchanged, when, under what authority, and for what purposes. As discussed in Option 1 of issue 7A, this approach would create a paper trail

but would not have the burdens attendant with formal process.

Option 2: Compulsory Process

For the reasons discussed in Option 2 of issue 7A, the Commission believed that compulsory process should be used for Federal access to state and local government records.

Option 3: No Paper Trail (Status Quo)

The arguments on this issue go primarily to the problems of compulsory process, rather than of letter head requests. Many government agencies, or components, do not have the legal authority to use compulsory process. Instead, they rely upon voluntary production of personal information by state and local agencies for the operation of programs, such as the security clearance and employment eligibility investigations. Although it is reasonable to expect that agencies would obtain individual consent for a state to release data, it is possible that an extension of the access limitation to state record keepers would endanger the present mode of operation of important Federal programs.

Decision:

_____ Letterhead request

_____ Compulsory process

_____ No paper trail

8. Should state and local government agencies be restricted in their information collection practices?

The Commission's access recommendations are aimed specifically at Federal agency activities, although the Commission's report states that, as a matter of policy and logic, its recommendations are equally applicable to state and local government agencies. However, out of concern for the difference in forms of state legal process and possible questions of constitutionality, the Commission did not include the information collection processes of state and local government agencies in its recommendations. Instead, the Commission stated that its proposals for reform of Federal government access should serve as a model for state action.

Although still undergoing extensive revision, including the possiblity of floor amendment on this issue, the bill under consideration by the House, and its companion bill in the Senate, apply the new access procedures only to Federal agencies. The Departments of Justice and the Treasury, however, have urged that the government access provisions be applied by Federal law to agencies at all levels of government seeking access to (bank) records.

There is a particular problem to be considered in deciding whether or not to extend the particular access provisions adopted for Federal agencies directly to the states by Federal law. The expectation of confidentiality, with its duty of non-disclosure for private sector record keepers, selected in Part II will prohibit informal access to records for all government agencies, state and local as well as Federal. Absent a Federal law reforming state as well as Federal processes, the loss of informal access would require state agencies to employ whatever forms of compulsory process they currently have available in order to obtain records. In many states this would impose little, if any, new burdens; in others, however, the end of informal access would leave state agencies needing access to personal records with few, and often very difficult, routes by which to obtain them. Furthermore, (1) establishing the expectation of confidentiality, (2) extending the particular government access provisions adopted earlier in this part only to Federal agencies, and (3) selecting the formal written request option in issue 1, could lead to the undesired side effect of placing a greater burden on state and local government agencies' access to records than on Federal agencies' access to those same records.

Three options exist with regard to the question of possibly extending the access provisions to state and local governments while at the same time avoiding the above-mentioned problem. The first two would retain the expectation of confidentiality and its concomitant duty on the record keeper not to disclose, unless required by law or permitted through legal process, as a barrier to informal access by agencies at all levels of government. In one case, the Administration could seek to directly extend the access provisions it decides to adopt for the Federal government to the states; in the other case, it could seek to expressly permit in statute the adoption by the states of new processes for access which incorporate at least the minimum protections

adopted for Federal agencies (e.g., incorporating at least the requirements for formal written requests, if that position was accepted in issue 1). The third option would be not to apply the access provisions for Federal agencies to the states and to eliminiate an individual's expectation of confidentiality when a state agency was seeking his records, thereby exempting the states from the restrictions on informal access to confidential personal information which were set forth in Part II.

Option 1: Apply access provisions to all levels of government

The philosophical and practical reasons that justify limiting Federal government access to records apply with equal force to state and local governments. Accordingly, a comprehensive approach assures the greatest protection of individual rights. In addition, a comprehensive approach avoids the dangers of: (a) inconsistent or conflicting state and Federal laws; (b) Federal-state preemption questions; and (c) "silver platter" investigations (i.e., investigations performed by a state agency that a Federal agency would not be able to perform legally, with a subsequent transfer of the fruits of the investigation to a Federal prosecutor.) By establishing one set of procedures and standards on a nation-wide basis, large national organizations and citizens of different states will be assured of equal and consistent treatment with regard to their legal obligations and rights.

There is considerable debate regarding whether this direct extension by Federal law of detailed access requirements to the states would be constitutional. Recent Supreme Court decisions indicate that the Federal government cannot directly legislate to alter or regulate the internal processes of state governments. There are, however, no constitutional obstacles to the creation by Congress of the expectation of confidentiality, and its concomitant duty on the record keeper not to disclose, under its authority to regulate interstate commerce. As noted above, once such a duty was in place, it could be expected to affect the circumstances under which state agencies obtain personal information, including the use of compulsory process. It would not, however, affect the internal procedures of state agencies or judicial systems. This is

the Justice/Treasury position. State agencies can be expected to oppose this position vigorously.

Option 2: Apply access provisions directly only to Federal agencies; permit, by statute, state adoption of processes with at least the minimum Federal requirements

The Commission did not look at state government access practices in as much detail as it looked at Federal government access practices and, hence, the factual record available to support extension of all the government access provisions to the states is not as complete. This option would, however, still establish a baseline national policy which would assure large record-keeping organizations and individual citizens of relatively consistent and equal treatment from state to state. In all likelihood, state laws adopted under this option would be similar, most likely following the Federal model.

Finally, this option avoids most of the problems of Federal-state relations inherent in the previous option and it limits the role of the Federal government in determining the investigative procedures of state agencies. For example, several states currently have more stringent requirements for access than are likely to be adopted by the Federal government. Application of a Federal law in those states could effectively lower existing state protections. By permitting, rather than directing, the adoption of lower Federal standards, this option leaves the final choice to the states. This is the Commission position.

Option 3: Apply access provisions only to Federal agencies; exempt state requests for records from the prohibition on informal access

This final option would create an exemption for state and local governments to the legally enforceable expectation of confidentiality defined in Section I.G.7. Its advantage is that it would avoid any potential problems by leaving the Federal government completely silent on state and local government access to records, but the cost would be the elimination of most of the protections for the individual provided by the expectation of confidentiality. In essence, there would no

longer be a consistent national policy protecting confidential personal records. On the Federal level, the elimination of restrictions on state agencies could result in records being made available to Federal investigators through state access capabilities which circumvent the intended protections of the Federal access requirements. (This concern is one of the arguments outlined above for direct application of the access provisions to all levels of government.)

Finally, this option would be viewed as creating a major loophole in any Administration privacy policy. There could be many different legally enforceable expectations of confidentiality, and, in some states, the individual could have no protection against state and local government access to records for which he had a legally enforceable expectation of confidentiality vis a vis Federal government access requests.

Decision:

_____ Apply all access provisions directly by Federal law to all Federal, state, and local government agencies.

__✓__ Apply access provisions directly only to Federal agencies; but expressly permit, by statute, states to adopt new access processes which incorporate at least the minimum protections for Federal agencies.

_____ Apply access provisions only to Federal agencies; exempt the states from both the particular access provisions for Federal agencies and the provisions of the legally enforceable expectation of confidentiality (as defined in Section I.G.7 and decided in Part II) which prohibit informal access by government agencies.

C. Compulsory Reporting Requirements

9. Should there be reform of compulsory record-keeping and reporting statutes?

All of the issues addressed above discuss access in the course of a specific investigation or administrative proceeding. This issue discusses those statutes which require the automatic and routine reporting of particular items of information by private sector record keepers (e.g., the Bank Secrecy Act) to the government. Because of the growing trend toward enactment of statutes that require private sector organizations to collect and maintain information about individuals for subsequent inspection by, or reporting to, government agencies, one of the Commission's Federal access proposals addressed the nature of these compulsory reporting statutes.

In particular, the Commission recommended that statutes that create requirements for private sector record keepers to collect personal information for inspection or reporting to government include the following provisions:

a) each requirement be expressly authorized in statute;

b) each requirement clearly identify the policies and purposes that it serves and establish standards by which to measure the relevance of the information required to these policies and purposes;

c) no information be collected or reported in individually identifiable form, except where necessary to accomplish a designated purpose and provided that the information is available for inspection by authorized agents of the government only upon presentation of a valid summons or subpoena;

d) each record keeper must notify an individual at the beginning of a record-keeping relationship of the information that government may see;

e) the information collected by the government is unavailable for unrelated civil or criminal prosecutions; and

f) the information is destroyed by the government, and may be destroyed by the record keeper, when and if the statute of limitations governing the use of such information expires.

Option 1: Commission Position:

The Commission concluded that these reforms were necessary

because the current system of record retention and reporting requirements "is fraught with greater potential for abuse, and threatens individual liberties and privacy more, than any other legitimate way government goes about gathering information." The Commission reached this conclusion on the basis of the following findings.

(a) Statutory grants of authority to agencies enabling them to require reporting or record keeping were ordinarily vague and overly broad, permitting agencies to establish requirements which result in the collection of information without appropriate attention to the agency's need for the information or to the utility of the information.

(b) Once collected, information flows relatively freely within government, with little attention to the propriety of such flow, particularly since the government need not justify the original compulsory collection and individuals are effectively barred from objecting to such "unreviewed executive discretion."

(c) The minimal agency restrictions on inspection of records that private institutions are required to maintain permit Federal agents' access to vast numbers of records without any need to justify their inquiry.

(d) "Few Americans are aware of the extent or nature of identifiable information about themselves reported to government or kept at government command."

(e) Information is kept beyond the time for which it is needed.

The crux of the Commission concern, in broad terms, lay in the exercise of "unreviewed executive discretion" in these information collection activities. The Commission decided that outside accountability must be recreated and that some standards need to be established setting limits to executive agency action and against which those actions can be measured.

Option 2: DHEW Position:

The Commission's proposal elicited two basic types of response from executive departments. The first type, typified by the response of the Department

of Health, Education and Welfare (HEW), endorsed the content of the proposal but indicated that the proposal should be implemented by broad statutory commands with the particulars left to agency regulation. The merit of this approach is that it would permit greater flexibility for the affected agency and allow for inclusion of necessary changes or amendments. On the other hand, the approach may fail to meet the underlying concern of the Commission, which was to minimize discretion in agency decision making and maximize the role of the Congress in establishing standards.

Option 3: Justice Position:

The second type of response, exemplified by the Department of Justice, agrees with HEW that regulation rather than statute should be the tool for implementation but further rejected the substance of the proposed limitation on use and redisclosure and on the imposition of a relevance standard. The Department of Justice believes that the Commission's recommendations would unnecessarily impede the flow of information used for law enforcement purposes. This concern may be mitigated, however, if the Congress were to endorse particular transfers in an applicable reporting statute. (The Department of Justice position here comes from task group #1, and thus is not linked to its testimony with the Department of the Treasury on bank records.)

Decision:

_____ Adopt the Commission position.

_____ Adopt the HEW position: endorse substance of Commission position but implement specific standards by regulation.

_____ Adopt the Justice position: reject limitation on uses and redisclosures and implement remaining substance of Commission position by regulation.

## IV. Federal Record-Keeping

This section addresses two general areas relating to privacy and the Federal government:

1) The record-keeping practices of the Federal agencies, particularly as they are covered by the Privacy Act of 1974, are candidates for re-examination in light of the Commission's findings; and

2) There are certain services provided by the government, particularly the provision of telecommunications and data-processing services for electronic funds transfer systems, which raise important privacy questions.

### A. The Privacy Act of 1974

Issue

The issue is whether the record-keeping and information management practices of the Federal government as they are covered by the Privacy Act of 1974 should be reformed. The Privacy Act has been criticized as a cumbersome and ineffective tool to solve real problems. While the principles of the Privacy Act are generally accepted, its specific requirements are believed by many to need improvement.

The Privacy Commission concluded that:

1) The Privacy Act represents a large step forward, but it has not resulted in the general benefits to the public that either its legislative history or the prevailing opinion as to its accomplishments would lead one to expect;

2) Agency compliance with the Act is difficult to assess because of the ambiguity of some of the Act's requirements, but on balance, it appears to be neither deplorable nor exemplary (in view of the ambiguity of the statute itself, the Commission was not prepared to judge agency compliance as either adequate or inadequate); and

3) The Act ignores or only marginally addresses some personal information record-keeping policy

issues of major importance now and for the future.

Also, criticism of the Act is often aimed at the lack of any significant, centralized rulemaking and policy making structure at the Federal level. It is believed that such a structure should, on an ongoing basis, consider how agencies would best administer the Act, as well as establish privacy policy for Federal programs which may face significant privacy problems not adequately treated by the Privacy Act. (This issue will be discussed separately in Part VI below.)

To the extent that these issues raise problems which demand immediate resolution, solutions may be possible through either legislative reform or unilateral executive action. Since the Privacy Act has been in effect for less than three years, there is a great deal of reluctance among congressional staff and Executive Branch employees to revise the Privacy Act legislatively at this time. Therefore, the discussion below presents alternatives for administrative, rather than legislative, action where they are practicable.

Current Law

The Act, in effect since September 27, 1975, requires agencies to:

1. publish a list of record systems they maintain on individuals, together with a statement of what the records are used for, to whom they are disclosed, and whether they are exempt from the access and correction provisions of the Act.

2. permit individuals to see and copy records about them, as well as to correct inaccuracies in those records;

3. limit the collection and use of personal information to that which is proper and necessary for an agency function;

4. limit the disclosure of personal information; and

5. ensure the reliability and security of personal information in their possession.

In addition to establishing these rights and obligations, the Act has certain definitional limitations to allow for exemptions. Also, the Privacy Act was drafted to allow for flexibility in the application of its provisions.

First, the Privacy Act does not cover all Federal records. Rather, it applies only to records which are retrieved by the reference to "name" or "other identifying particular." The intent was to impose the Act's requirements on records about particular individuals which were maintained or used on an easily retrievable basis.

Second, the Act, drafted to satisfy the concerns of many government officials, particularly those representing law enforcement, provides a very broad exemption structure in which entire record systems may be excluded from many of the Act's provisions. Congress recognized that ongoing law enforcement investigations, certain personnel evaluations, and legitimate national security interests could be jeopardized by disclosure of certain records. It sought, by exempting complete systems containing such records from the individual access and certain other provisions, to protect the government from premature exposure of such operations.

Third, in applying through specific statutory provisions the general principle of limited disclosure of personal information, Congress recognized that it still could not identify in the statute every disclosure which was appropriate for each Federal agency. To ensure the continued flow of needed information among agencies, while providing some protections against indiscriminate disclosure, the Congress established a "routine use" provision which permits an agency to freely disclose information outside of the agency when the disclosure is for a use "compatible with the purpose for which (the record) was collected." Also, none of the Privacy Act's limitations on disclosure apply to personal information that is required to be publicly disclosed pursuant to the Freedom of Information Act.

Fourth, in the interests of flexibility and decentralized administration, Congress elected to allow agencies to tailor implementation of the Act to their particular needs and responsibilities. While the Office of Management and Budget (OMB) was given some authority to issue guidelines and provide direction, such guidance is not binding on the agencies; nor is government-wide regulatory or enforcement authority given to any other organization.

Finally, to enforce compliance with certain provisions of the Act or to recover actual damages occasioned by an "intentional or willful" violation, an individual may sue an agency directly. An individual may compel the agency to allow him access to a record about him, or to correct that record, as well as recover his out-of-pocket expenses.

Discussion

The Commission concluded "that the Privacy Act needs significant modification and change if it is to accomplish its objectives within the Federal Government." The specific findings which led to the call for general overhaul of the Act are too numerous to list, but a sample should indicate the breadth and complexity of what the Commission believed were the principal problems with the Act. The Commission found that:

1. The current use of the Act's "system of records" definition allows agencies to avoid the requirements of the Act by changing the way their records are retrieved. Some agencies have, in fact, changed certain retrieval schemes in order to avoid the Act's requirements;

2. The Privacy Act's approach to exemptions from the individual access requirement permits a situation where access could be denied under the Privacy Act, because the record belonged in an exempt system, but allowed under the Freedom of Information Act, because its release would not jeopardize any legitimate law enforcement or national security interests (with one consequence being that the individual could see the record but not correct it, since the Privacy Act's correction rights did not apply); and

3. The "routine use" provision of the Act is being interpreted so broadly by most agencies that it encompasses almost any disclosure of information to parties outside the agency. Also, it provides no standards for internal agency disclosures, even where the disclosure would be between two otherwise unrelated components of a massive agency, such as DHEW (e.g., between the Social Security Administration and the Public Health Service).

The Privacy Commission made a number of suggestions which, when taken together, constitute a wholesale revision of the existing Act. The Commission also prepared a model statute embodying its strategy for revision of the Act; that model statute has been introduced in the House as H.R. 8279 and as one portion of H.R. 10076. The Commission proposals include several steps it believed essential to any revision of the Act;

1. The ambiguous language in the law should be clarified to minimize variations in interpretation.

2. Clarification of the Act should explicitly incorporate "reasonableness tests" to avoid a strict interpretation of the Act and to allow for flexibility in implementation. This would give the agencies incentives to attend to implementation issues and to take account of the differences between manual and automated record keeping, diverse agency record-keeping requirements, and future technological developments.

3. The Act's reliance on its "system of records" definition as the sole basis for activating all of its requirements should be abandoned in favor of an approach that activates specific requirements as warranted. (This is a fundamental change in the basic structure of the Act, and it reflects the generally accepted view that real reform of the Act will require changes in the Act's definitions.)

4. Provisions should be incorporated into the Act which would increase agency accountability and ensure more effective application of the requirements of the Act--through better implementation, more vigorous oversight, and more thorough and effective enforcement of the Act.

Issues for Decision

1 Should the Administration endorse revision of the Privacy Act?

Pro:

The Privacy Commission concluded that the Act, while a large and worthwile step forward, was

not meeting its objectives, and many observers both in and out of government agree. It is certainly possible to improve the Act while reducing the current burden on the agencies. In addition, there is some doubt as the legitimacy and credibility of agency objections to revision of the Act based on claims of burden. The concerns expressed by the various agencies at the time of the Act's passage regarding cost of implementation and burden of administration have generally proved unfounded. Indeed, original agency estimates of cost were too high by a factor of almost 10.

The Presidential policy regarding privacy protections for the private sector may be difficult to justify and may suffer in credibility unless there is a concurrent effort to further reform Federal record keeping. Further, to the extent that the Privacy Act serves a a model for state legislative action, any fundamental weaknesses may be carried over and duplicated.

In the international arena, there is pressure to revise the Privacy Act to cover all individuals instead of just American citizens. While this is thought to be a simple modification, it can be expected that such a move would, at a minimum, call into question the entire exemption structure of the Act.

Con:

The arguments against revision of the Privacy Act are generally not based upon support for the structure or effectiveness of the current law as much as they are based upon the inadvisability of taking any action at this time because: (1) there is not enough data available to justify and guide a revision effort; and (2) there is little political support for revision of the Act.

The Privacy Commission's specific suggestions for revision of the Act were presented in a different format from the other, more general, recommendations in the Commission's report. The agencies were not tasked to respond to these specific legislative suggestions as part of this review process, and most did not do so. Based upon the limited information available, however, it can be expected that agency reaction will be strong and widely varied in relation to the specific language of any proposed revision

of the Act. Those agencies which did respond expressed concern over increased costs of implementation and expanded administrative burdens, as well as over the possibility that certain of the proposals, if adopted, would prove unmanageable, notwithstanding any concern over burden and expense.

In addition, there is little discernible support, either in the Congress or in the agencies, for massive revision of the Privacy Act at this time. Even those who would strengthen the Act are fearful that opening it up to amendment now may do more harm than good. The general inclination is to wait and see how the Congress deals with other areas of privacy, principally as regards government access to private sector records and general private sector record keeping, before attempting any restructuring of Federal sector record keeping.

Compromise:

There exists a middle position between endorsement of the Privacy Commission proposals for complete revision and rejection of basic reform of the Act. The Administration can endorse broad reform but not commit itself to the specifics or methodology adopted by the Privacy Commission. Since the Commission's investigation occurred in the earliest days of the Act's life, it may be wise to examine the subsequent experience before endorsing specific revisions. As part of this reform, it might also be appropriate to take certain steps administratively (as discussed further below).

Decision:

_____ Endorse Privacy Commission recommendations to fundamentally revise and strengthen the Act.

_____ Endorse concept of fundamental revision of Act in 1979-80 Congress with goal of strengthening Act while minimizing agency burden; assign staff to review issues and develop positions.

_____ Defer fundamental changes in Act until there is more experience under it; plan tentatively to seek legislation in 1981.

Whatever the decision on legislative reform, there are certain steps which do not require legislation and may be taken administratively, regarding certain of the Commission's recommendations:

2. Should the applicable provisions of the Privacy Act apply to records generated by Federal funds, for use by the Federal government (i.e., should recipients of discretionary Federal grants be included under the Act)?

This extension could be implemented by requiring agencies to incorporate the appropriate parts of the Privacy Act into their grant instruments. Generally speaking, this provision would cover research grants.

The provisions of the Act would not be extended, however, to employment, personnel, or administrative records which the grantee maintains as a necessary aspect of supporting the grant, but which bear no other relation to its performance. The provisions of the Act also would not apply to individually identifiable records to which the following three conditions apply: (1) records that are neither required nor implied by terms of the contract or grant; (2) records for which no representation of Federal sponsorship or association is made; and (3) records that will not be provided to the Federal agency with which the grant is established, except for authorized audits or investigations. The specificity in delineating which records are covered represents an attempt to preserve the intent of the Act while removing some of the confusion that could result in undue burden on grantees.

Pro:

The Privacy Commission concluded that records about individuals generated either in response to Federal needs or with the assistance of Federal recources should be afforded the basic protections of the Act. The Act currently applies in this regard to government contractors. In general, the Executive agencies agree with this proposal.

Con:

HEW believes that such extension will lead to increased costs and administrative burdens for grantees, burdens which will ultimately diminish the resources available under any particular grant

which generates or uses personally identifiable records,

Decision:

_____ Extend provisions of Act to recipients of discretionary Federal grants administratively.

_____ Do not extend Act.

3. Should the "routine use" provision of the Act be substantially strengthened?

This decision could be implemented through Executive order or revision of OMB guidance.

Pro:

The "routine use" provision is viewed by most observers as a major weakness of the Act, permitting agencies great and unintended latitude to disclose personal information while still allowing them to uphold the letter of the law. The Commission advocated a substantial tightening of the "routine use" provision of the Act for two reasons: (1) agencies have interpreted nearly all external disclosures of information as "compatible with the purpose" for which the information was originally collected; and (2) the clause provides no standards for internal agency disclosures.

In order to correct these problems, the Commission proposed that any decision to establish "routine" uses or disclosures of personal information should be required to meet an additional test for consistency with the "conditions or reasonable expectations of use and disclosure under which the information was provided, collected, or obtained." Such a provision would enable an individual to measure the subsequent use of his personal information against the expectation he had when he supplied it, as opposed to simply any technically legitimate purpose for which the information might be employed, whatever the original expectations of the individual or agency. This would afford individuals with an increased measure of control over their records.

Con:

In response, the agencies generally argue that, while such a test, and its imposition on both

external and "internal" disclosures of information, would go a long way toward solving the problems identified by the Commission, it would also impose a significant burden. Further, it could pose the risk that agency judgments might come under legal scrutiny on the basis of the subjective expectations of an individual at the time information was collected, although clearly drafted notices to the individual at the time of information collection (already a Privacy Act requirement) would presumably address this concern. The proposal would also eliminate the broad and, agencies argue, Congressionally intended agency discretion over how information will be used and disclosed internally.

Compromise:

Given the considerable latitude provided by the current "routine use" provision, the Administration could adopt the position that the "compatible purpose" test needs to be revised, although not necessarily with the standard proposed by the Commission. This approach would provide affirmative Administration action on what is viewed as one of the major deficiencies of the Act. At the same time, it would avoid the problems of the legislative process and a possibly reluctant Congress. Also, OMB is currently circulating draft guidelines on the sharing of information between agencies for use in "matching" programs. These guidelines would be a solution to one segment of the "routine use" problem.

Decision:

_____ Revise the "routine use" provision along lines recommended by the Commission.

_____ Accept concept of revising "routine use" standard; instruct staff to develop alternative to Commission's approach.

__✓__ Take no action (i.e., retain current "routine use" standard).

4. Should a position be created within each agency to oversee implementation of the Privacy Act?

Pro:

The Privacy Commission found that agencies which experienced the greatest success in implementing the Privacy Act had established formal mechanisms to deal with its requirements. The Commission believed that a critical element in this approach was the designation of one responsible official with authority to oversee the Act's implementation, and the Commission therefore recommended designation of such an official in every agency. This official's responsibilities would include: (1) issuing any instructions, guidelines, or standards necessary to implement the Privacy Act; (2) assuring the consistent application of regulations and policies within the agency; and (3) providing for the effective education of system managers and decision makers who are responsible for the collection, maintenance, or disclosure of personal information. This proposal, which could be adopted as a matter of Presidential directive, would strengthen the basic non-centralized enforcement strategy of the Act. The agencies have almost universally endorsed this suggestion.

Con:

No counterarguments have been presented.

Decision:

_____ Adopt Privacy Commission proposal to create an agency position to oversee implementation of the Privacy Act.

_____ Take no action.

5. Should the processes of internal agency oversight in the development of new systems for the use and storage of personal records be reformed?

Federal agencies have been criticized for the process they use to decide such questions as how to configure their record-keeping systems and what computer/communications systems to develop and deploy. It is argued that these decisions too often are made at the operations level, with inadequate policy oversight and consideration of privacy and other social implications. Considerable time, money, and effort have been spent in recent years designing and perfecting automated record-keeping systems which have subsequently been halted in the final stages

of development when Congress or others have discovered a lack of consideration for privacy and other individual rights in the system design. In addition to the costs incurred, this eleventh-hour delay or cancellation of systems leads to the loss of needed information resources by agencies and causes frustration and lowered morale among those who plan and develop these new systems.

There is thus an issue of whether or not to reform the existing processes for oversight of system development to assure that the earliest possible consideration is given to privacy protection and similar concerns. Part of the needed reform may be the establishment of a centralized oversight function for the Executive Branch, a possibility explored in Part VI below. Another step in resolving this problem may be to establish more effective policy oversight and review within each agency. The following options present possible mechanisms for achieving these goals. The options are not, however, mutually exclusive; all or any combination of them could be adopted.

Option 1: Assign oversight and review responsibilities to a designated agency official.

Responsibility for reviewing proposed new systems, or changes to existing systems, early in the planning stages could be assigned to the designated agency official (discussed in issue 4 above). He could assist in new systems design by examining proposals with regard to their impact on personal privacy. Because this official would be responsible for all privacy-related matters within the agency, he would be more sensitive to these interests than those with purely program or system development responsibilities.

Option 2: Establish guidelines on the responsibility, training, and appointment of system managers.

The Privacy Act requires that a "system manager" be named for each proposed new system. Agencies have varied widely in their interpretation of this requirement; system managers range from senior agency officials to computer technicians. Guidelines could be issued, presumably by OMB, requiring, for example, that the system manager be named at the beginning of the process of planning the system, that he be someone with knowledge of the system, and that he report directly to the person

running the agency program which the system serves. In addition, agencies could be required to develop, or augment existing, programs for educating system managers in the broad policy objectives of designing and operating systems which incorporate concerns such as privacy.

This option would help to increase accountability within each agency for system design, development, and operation. It would establish a clear line of authority between the operators of systems and decision makers using them, which should make the decision makers more aware of potential problems in system design and development. This option would also increase the effectiveness of system managers in identifying and alleviating potential privacy problems.

Option 3: Adopt earlier trigger mechanisms for external oversight.

As now required by the Privacy Act, the "trigger" for external oversight of a new record-keeping system is preparation of a new system notice which is sent to OMB and the Congress. By this time, however, an agency usually has spent substantial sums designing the system and is committed to it. This lessens the likelihood that the privacy issues which will be raised by outside reviewers can be readily resolved. Agencies could be required to prepare these notices earlier in the design stages of the system or, alternatively, to prepare an annual agenda of the major systems under consideration and forward the agenda to whatever agency has central Executive Branch oversight authority for review.

Decision: (Any number of those options may be selected)

_____ Assign oversight and review responsibilities to the designated agency official.

_____ Establish guidelines on the responsibility, training, and appointment of system managers.

_____ Adopt earlier trigger mechanism for external oversight.

B. Federal Provision of Data-Processing and Telecommunications Services: Electronic Funds Transfer

Issue

The Federal government, less by deliberate design than by circumstance, has become increasingly involved in the provision of data-processing and telecommunications services to state and local governments and even to private organizations. The provision of these services by the Federal government raises a broad range of policy questions, among them privacy issues. Moreover, these issues are fundamentally different from the others considered in this memorandum. They go to the structure of government in an information society. The concern is that, if government itself provides telecommunications and data-processing services for personal information, then government will have direct and unaccountable access to it. It will thus become significantly more difficult to enforce whatever privacy protections the society decides to adopt.

This memorandum seeks decisions only in relation to the Federal government's provision of Electronic Funds Transfer (EFT) services. (An earlier memorandum from the President's Reorganization Project dealt with a similar problem concerning the FBI's operation of certain telecommunications services through NCIC.) The specific question to be addressed here is what the role of the Federal government should be in the operation of EFT systems. In particular, what restrictions, if any, should be imposed on government operation of EFT systems, and what privacy protections should be established in those circumstances in which government does provide EFT services?

Discussion

The term Electronic Funds Transfer (EFT) encompasses a number of financial services which generally involve moving funds from one depository account to another, without also moving pieces of paper. In order to understand the privacy issues engendered by EFT, a brief description of the paper check system and of several EFT systems is appropriate.

When a check drawn on one bank is deposited in another bank, the bank receiving the deposit must arrange to have that check physically transported to the bank on which it was drawn. In some cases, two banks will directly exchange checks drawn on each other. Where

a number of local institutions are involved, they will all meet at a designated time and place each day and exchange checks. The place where they meet is called a clearinghouse.

When the check is drawn on an out-of-town bank which is not a member of the local clearinghouse, the bank will frequently present the check to the Federal Reserve System for collection. The Federal Reserve will transport the check directly to the out-of-town bank (or to a processing center designated by that bank). The Federal Reserve System currently clears approximately 40% of all checks. Although computers may be used to process the checks, the payment instructions are still written on paper (i.e., the check) and, hence, this form of financial transaction can be called Paper Funds Transfer.

In Electronic Funds Transfer, by contrast, the payment instructions that in the check system are contained on the paper check are instead represented electronically. The electronic message may move instantaneously from a terminal at a merchant's checkout counter to the customer's bank and result in the instantaneous transfer of funds, or it may be written on a magnetic computer tape for later posting to the appropriate account. The critical element from a privacy standpoint is that the payment data is contained in a machine-readable form and, in some systems, is transmitted electronically to a central location.

There are several forms of Electronic Funds Transfer systems, the most important for the purposes of this memorandum being the automated clearinghouse (ACH) and the point-of-sale (POS) system. An automated clearinghouse is an outgrowth historically of the paper check clearinghouse discussed above. Just as banks bring paper checks to a traditional clearinghouse, banks (or other depository institutions, such as savings and loan associations, mutual savings banks, and credit unions) that participate in an ACH bring to it a magnetic computer tape containing payment instructions concerning their customers' accounts. The ACH processes these tapes, sorts the payments by receiving bank (the bank in which the person or company receiving payment has its account), and sends each bank a new computer tape containing payment instructions for its accounts. In most cases today, the tapes are transported physically, although for transfers between different ACHs and between ACHs and participating financial institutions, systems have been developed to transmit the data

electronically via a telecommunications link instead of manually through the exchange of computer tapes.

An ACH payment begins when an individual signs the paper authorizing the transaction--for example, authorizing his employer to deposit his wages automatically, or authorizing his insurance company to deduct insurance premiums automatically. Following this initial written authorization, the transfers continue to occur on a regularly scheduled basis until the individual revokes the authorization (or loses his job or his insurance coverage). Because of this initial authorization process, ACHs are currently used primarily for large, regularly recurring payments, such as salary, social security, annuity, insurance, or mortgage payments.

A second example of EFT is the point-of-sale system in which the purchaser, using a terminal that is located at a merchant's establishment and is electronically connected to the customer's depository institution, transfers funds instantaneously from his depository account to that of the merchant at the time of purchase. Unlike ACH transactions, POS transactions are not pre-authorized and regularly recurring. Each transaction is individually initiated by the customer for an amount of money that varies with the purchase, much like a credit-card transaction. There are very few POS systems in operation, although this is the system most people have in mind when they think of EFT.

Finally, there is also a hybrid POS/ACH system that is technically feasible and may be economically attractive but that does not yet exist. In this system, the POS terminal at the merchant location (or the bank computer to which the merchant terminal was electronically linked) would record the transaction on magnetic tape. The magnetic tape would then be processed at the end of the day through an ACH.

Depository institutions are developing EFT systems for a number of reasons. First, EFT transactions are accomplished without a visit to the depository institution or the execution of a check, thus saving time and the cost of processing slips of paper. Second, payment is assured, thereby avoiding problems occasioned by the reluctance of merchants to accept personal checks. Finally, because EFT allows all depository accounts to be subject to withdrawl on demand, like present-day checking accounts, funds in all types of depositories--commercial banks, savings and loan associations, mutual savings banks, and credit unions--may be utilized.

The Privacy Commission believed that the EFT systems that create these benefits also raise problems for individual privacy. The sheer efficiency of electronic transfer, as opposed to manual paper transfer, dictates that the records will become more centralized and the details more easily retrievable for outside use than they are today. It is far simpler to retrieve transaction information through the use of computers than by a physical search of paper or microfilm/microfiche records. Also, point-of-sale services increase the potential for monitoring an individual's movements and activities, since they create a real-time record of his financial transactions.

Moreover, the Privacy Commission concluded from its study of EFT that continued development will result in the recording of more detailed information about individuals by financial institutions than is otherwise required, including, perhaps, items of information not ordinarily considered payment data. For example, accounting and administrative data, such as benefit and tax withholding information, may eventually accompany the strictly financial data now maintained by depositories.

Current Law and Practice

The Federal government is currently engaged in widespread, and growing, use of electronic funds transfer to make government payments for salaries, pensions, revenue sharing, and the like. One of the nation's major currently operating EFT systems, the ACHs discussed above, is operated by a Federal agency, the Federal Reserve Board, which provides this service both for the Department of the Treasury and for private sector institutions. If, for example, a private employer wishes to use EFT to pay its employees, or to receive payments from its customers, the payment information flows through the Federal Reserve. Government payments are still the great majority of all ACH transactions, but the share initiated by the private sector is growing.

There are now 32 ACHs in operation: two run primarily by the private sector, 30 by the Federal Reserve. The Federal Reserve recently decided to link these ACHs through a Federal Reserve-run telecommunications system, so that information flowing between ACHs will move electronically through a government telecommunications system.

At present, the Federal government does not process point-of-sale (POS) transactions. However, as POS

systems (and other EFT systems, such as telephone bill paying) increase and penetrate new markets, the natural progression may be for ACHs to clear these transactions as well. It is this information which the Privacy Commission believed could form the raw material for piecing together personal profiles of individuals.

Federal law has not yet addressed the special policy issues arising from the development of EFT systems. There are, however, bills currently in both the Senate and the House focusing on the privacy questions of EFT and the numerous other issues raised by these systems.

Areas of Agreement

There is agreement that privacy protections for EFT should include, in addition to the provisions generally applicable to depository institutions, the following:

1. Individually identifiable account information generated in the provisions of EFT services should be retained only in the account records of the financial institution and other parties to a transaction, except that it may be retained by the EFT service provider to the extent, and for the limited period of time, that such information is essential to fulfill the operational requirements of the service provider;

2. Procedures should be established so that an individual can promptly correct inaccuracies in transactions or account records generated by an EFT system, so as to provide protections for EFT systems comparable to these provided by the Fair Credit Billing Act for credit-card systems.

3. With respect to government-operated systems: (Note: provisions 3(a) and (b) below are recommendations of the National Commission on Electronic Fund Transfers, and have been considered only by the 12 Federal agencies represented on that Commission, rather than by all the agencies involved in this review process.)

   a) Any government agency providing EFT services should follow privacy rules and procedures that are at least as

restrictive as those of private sector EFT system operators; and

b) Access by other government agencies to records of EFT transactions in the temporary possession of a government EFT service provider should be governed by rules and procedures that are at least as restrictive as those for access to EFT records maintained by private sector financial institutions.

Issue for Decision

1. Should the Federal government withdraw from, or restrict its operations of, EFT services for the private sector?

Option 1: Do not limit government operation of EFT for the private sector at this time.

To date, private sector depositories have not provided ACH services without the Federal Reserve's operational assistance. The Federal Reserve System has operated an electronic funds transfer network since 1918, over which transactions in Federal Funds, U.S. government securities, and settlements between commercial banks are effected. More recently, as commercial banks have experimented with the exchange of payments on magnetic tape, rather than by paper check, the Federal Reserve has performed clearing and settlement services for these payments similar to those it does for payments made by paper check. (The Federal Reserve today clears about 40% of all checks.)

The Federal Reserve has shared ACH research and development costs with the private sector, and operates 30 of the 32 ACHs. It can be argued that only Federal Reserve operation permits nationwide availability of ACH services at this time. Thus, significant economic consequences may result should government participation be constrained.

A second concern is that the U.S. Treasury has determined that the cost of disbursement could be lowered by converting government payments from check to magnetic tape. The Federal Reserve, as the Treasury's fiscal agent, distributes these payments along with the paper check payments that

it has traditionally distributed for the Treasury. Thus, regardless of whether or not alternative private systems develop, the Federal government will continue to provide these services for its own payments. It is argued by some that since the marginal additional cost to the Federal government of also providing these services to commercial banks is minimal, government should continue to do so at this time.

Finally, it is argued that the Federal Reserve's sixty year history of handling paper checks and electronic transfers of Federal funds, as well as its more recent operation of ACHs, has shown no abuse of the information as a result of Federal Reserve operation. Furthermore, while an automated clearinghouse does not today collect or transmit enough data on individuals to permit a significant infringement on personal privacy to occur, the Federal Reserve is currently taking affirmative steps to increase protection for the privacy of the transaction data processed by the automated clearinghouses that it operates. It is thus argued that to cease providing this service for private sector organizations could have a harmful effect upon the cost to the private sector of making payments, without a corresponding increase in the protections of privacy. This option is supported by the Federal Reserve, the Department of the Treasury (which believes further study is required and that the determination should not be made in the context of the privacy issue alone), the U.S. Postal Service, and the General Services Administration (which agrees in principle with Option 2, but believes that that option is too broadly drafted, and therefore supports Option 1).

Option 2: Provide that no government entity be allowed to own, operate, or otherwise manage any part of an electronic payments mechanism that involves transactions among private parties.

The Privacy Commission recommended this position because it believed that, as EFT services "become more sophisticated and documentation and surveillance capability increases, government's operation of EFT systems will become...an unparalleled threat to personal privacy," far greater than the threat

posed by the current, relatively unrestricted government access to bank records. If the Federal Reserve were to operate point-of-sale (POS) systems directly, or if a variety of POS systems were to develop, as some have suggested, in which the individual transactions that occurred during a day were captured on computer tape and later batch-processed through government operated ACHs, then government's ability to monitor individual behavior, it is argued, would be significantly enhanced.

In addition, a government operated and subsidized system makes it less likely that private sector alternatives will develop, leading to a greater concentration of financial information than would otherwise occur. Further, "government as operator" is in a conflict of interest with "government as regulator," making it less likely in the future that necessary but possibly inconvenient privacy protections will be imposed on the developing EFT systems. Finally, the Privacy Commission concluded that the organizational structure for EFT is developing so rapidly that unless a decision to limit government operation is taken now, "the inertia of economic circumstance may destroy the policy choice, leaving the Federal Reserve as the basic provider of service."

Option 3: Allow government operation of automated clearing-houses (ACHs), but not, at present or in the foreseeable future, of point-of-sale (POS) switching and clearing facilities, except for the provision of net settlement among depository institutions.

Automated clearinghouses do not collect or transmit enough data on individuals to permit a significant infringement on personal privacy. The payments now being transmitted by ACHs are primarily recurring payments such as salary, insurance, and mortgage payments, plus payments such as revenue sharing that do not involve an individual's account. Government operation of ACHs, therefore, poses no insurmountable privacy problems. Point-of-sale systems, by contrast, may collect, transmit, and store sufficiently detailed information on an individual's behavior to allow the creation of a detailed portrait of his activities and beliefs. Allowing government to operate POS switching or clearing facilities could, in a mature EFT system,

put a government agency at the heart of a data-communications system containing detailed personal information on the citizens using the POS systems.

There is no significant impetus, either within government or from the private sector, for government to begin operating POS systems. Permitting government to continue operating ACHs, while forbidding government to provide anything other than net settlement for POS systems, would provide a compromise which protects privacy but does not disrupt current EFT operations. This was the recommendation of the National Commission on Electronic Fund Transfers, and is supported by the National Credit Union Administration and the Commerce Department.

Decision:

_____ Do not limit government operation of EFT for the private sector [at this time].

_____ Provide that no government entity be allowed to own, operate, or otherwise manage any part of an electronic payments mechanism that involves transactions among private parties.

_____ Allow government operation of automated clearinghouses (ACHs), but not, at present or in the foreseeable future, of point-of-sale switching and clearing facilities, except for the provision of net settlement among depository institutions.

V. Other Issues

A. The Use of Truth Verification Devices in Employment

Issue

Truth verification devices are used to try to determine whether or not someone is telling the truth by examining changes in a person's physical characteristics thought to be beyond his voluntary control. The question is whether there should be a Federal law to forbid a private sector employer from using the polygraph or other truth verification devices (e.g., the Psychological Stress Evaluator) to gather information from an applicant or employee? This issue does not address the use of these devices in the law enforcement context, since the courts now deal with these questions by determining the admissibility of polygraph tests as evidence in criminal trials.

Current Law and Practice

Civil Service Commission regulations prohibit the use of polygraph and other truth verification devices in Federal employment. Where their use in private employment has been regulated, regulation has been by the states. A few states ban their use entirely; most either only license their operators or do not regulate them at all. Senator Bayh has introduced S. 1845 to prohibit the use of these devices for private employment purposes. Hearings have been held.

Employers currently use truth verification devices in two contexts. First, some employers administer tests when an individual applies for employment, and on a regular schedule to current employees. Second, the devices are sometimes used to gather evidence about employees suspected of illegal activity on the job.

In 1974, about 300,000 private-sector employees were tested.

Issue for Decision

Should Federal law prohibit the use of polygraph and other truth verification devices in employment?

Pro:

This is the Privacy Commission proposal, and is supported by the Department of Labor. Objections

to the use of truth verification devices go to their inherent intrusiveness, and to their effect of depriving an individual of control over divulging information about himself since he generally must submit to the test or lose his job. Unions have alleged that these devices are used more to frighten employees than to get information. Moreover, there is some question as to the reliability of these devices. In the main, truth verification devices are not considered sufficiently reliable for the results obtained by their use to be admissible in court. In response to these concerns, many major employers have ceased to use them.

Con:

Opposition to this proposal comes from private business, particularly the retail industry. They argue that a prohibition on polygraph and other truth verification devices will increase the cost of employee theft and fraud, and that this cost will be passed directly to the consumer and society. In addition, it is argued that the impact will fall most heavily on smaller businesses which are at a competitive disadvantage in absorbing these costs.

Decision:

_____ Yes, prohibit the use of polygraph and other truth verification devices in employment.

_____ Take no position.

_____ Oppose Federal legislation.

B. Standard Personal Identifier

Issue

It is a common perception that when a government assigns a number to each of its citizens it can then track an individual through every aspect of his life. It is an equally common belief that the absence of a unique and standard personal identifier would make such a task more difficult. The continuing advancements in computer technology have served to magnify such concerns. Finally, many individuals see the general use of the Social Security Account Number (SSAN) as a real threat to their personal privacy; indeed, such usage has become a symbol for many privacy problems.

Discussion

The Privacy Commission, following a detailed study of the use of SSAN, concluded, as have most other groups studying the problem, that a Standard Personal Identifier system is less a problem than it appears to be. The Commission further concluded that the real problem is the exchange of information among record systems. A Standard Personal Identifier would facilitate such exchanges. However, the absence of a Standard Personal Identifier does not now significantly restrict this flow of information.

Modern technology has already sidestepped the need for a single, unique number which identifies individuals. With nothing more than name, birthdate, birthplace, and address, it is possible to accurately identify an individual or his record. As a result, most observers agree that the more appropriate method for dealing with this problem is to develop safeguards and protections against the unrestricted flow of personal information, generally along the lines suggested by the Commission for the agencies.

Any statement of Administration privacy policy must, however, remain sensitive to the public concern over the Standard Personal Identifier issue. It must also be adopted with the understanding that the privacy problems encountered with the Standard Personal Identifier are inherently without solution. This is because, in the privacy context, the strength of a Standard Personal Identifier is also its weakness.

The use of a Standard Personal Identifier certainly facilitates the exchange and consolidation of records

or information about an individual. By the same token, however, it also ensures accurate personal and record identification in all instances and serves to minimize errors in the transfer of information and documents both inside and outside an organization. Without the accuracy a Standard Personal Identifier supplies, an individual might be denied a right, benefit, or opportunity to which he would otherwise be entitled. The time required to gain access to information is significantly reduced, which increases organizational efficiency and decreases costs to the taxpayer or consumer. The Commission concluded that accurate personal and record identification are an essential component of fairness in record keeping.

The aspects of a Standard Personal Identifier system which allow these benefits to flow give rise to serious concern among members of the public, however. The same records management systems which are aided by the Standard Personal Identifier in the exchange and consolidation of all personal information about an individual can be manipulated to produce the identical result for illegal or improper purposes. Certainly, information held by one record holder should not in all instances be made available or accessible to another decision-making record holder. And yet, the Standard Personal Identifier would facilitate and, some would argue, encourage just this type of information "swapping" between record holders.

Finally, there is opposition to use of the SSAN, or any Standard Personal Identifier, on the grounds that it tends to dehumanize people, reducing them to their SSAN, or whatever other number is assigned. While the depth of this feeling is undeniable, it is not clear that there are any real policy choices to deal with it. Removal of all the account numbers that people possess in today's society is simply not a realistic option.

Current Law and Practice

Section 7 of the Privacy Act of 1974, P.L. 93-579, was intended to control the use of the SSAN as a form of Standard Personal Identifier. That section makes it unlawful for any Federal, state, or local governmental agency to deny an individual any right, benefit, or privilege based upon his refusal to disclose his SSAN. Such prohibition, however, does not apply in those instances where disclosure is required by Federal statute

or where the requirement existed prior to January 1, 1975. Further, any agency requesting such disclosure must inform the individual whether his disclosure is mandatory or voluntary, the authority under which solicitation is made, and the uses that will be made of the SSAN.

In the Federal sector, the impact of this section has been limited by Executive Order 9397, which was promulgated in 1943 and which instructs agencies to use the SSAN when establishing new systems of account numbers. This order has been interpreted as constituting a requirement in existence prior to January 1, 1975, and, consequently, as continuing authority for the use of the SSAN in new record systems. A further limitation on the proscriptions outlined in Section 7 of the Privacy Act is to be found in the Tax Reform Act of 1976. In that statute, any state or political subdivision thereof is authorized to require disclosure of the SSAN and to rely on it as a personal identifier in the administration of any tax, general public assistance, driver's license, or motor vehicle registration law. As a consequence of Executive Order 9397 and the Tax Reform Act, the already widespread use of the SSAN as a standard identifier in the public sector is not significantly limited.

Use of the SSAN in the private sector is somewhat more limited. This is partially due to the fact that most large commercial organizations assign their own particular number to each individual's account or record. It is also due to the ability of modern computer systems, as discussed above, to accurately identify an individual or his record without placing reliance on a particular number. As an example, one large credit information organization with over 50 million records in its system routinely identifies individual records based on nothing more than name, address, and date and place of birth.

Areas of Agreement

There is agreement among the Commission and the agencies on the following points concerning privacy protections for a Standard Personal Identifier:

a) the Federal Government should do nothing to foster the development of a Standard Personal Identifier until it has addressed the underlying issue, which is controlling the disclosure and exchange of recorded information; and

b) the limits currently placed by Section 7

of the Privacy Act on the use by Federal, state, and local government agencies of the Social Security Account Number as an identifier should not be increased.

Areas of Disagreement

1. Should Executive Order 9397 (a 1943 order directing Federal agencies to use the Social Security Account Number when establishing a new system of permanent account numbers) be amended so that Federal agencies may not, as of January 1, 1977, rely on it as legal authority by which to create new demands for the disclosure of an individual's Social Security Account Number (SSAN)?

Pro:

The Commission believed that use by some agencies of E.O. 9397 as legal authority for requiring disclosure of the SSAN undercuts the intent of the Privacy Act's Section 7. The Commission believed that Section 7's exemptions were intended to apply only where an agency has specific legal authority to require disclosure of the SSAN, and not when it has an authority of general applicability such as E.O. 9397.

In order to minimize disruption, the Commission recommended that agencies that had relied on E.O. 9397 as authority to require disclosure of the SSAN before January 1, 1977, should be allowed to continue to do so.

Con:

The agencies oppose this recommendation as being disruptive and of little benefit at this stage. In the Department of Defense, for example, virtually all computerized records are indexed on the basis of SSAN.

A prohibition on the future use of the SSAN would require the maintenance of separate, and different, indexing programs, with questionable beneficial results.

Decision:

_____ Yes, amend E.O. 9397 so that Federal agencies may not, as of January 1, 1977, rely on it as legal authority by which to create new demands for the disclosure of an individual's Social Security Account Number.

_____ No, do not amend E.O. 9397.

C. Research and Statistical Studies

Issue

In the Privacy Commission's view, the use of personal records for research and statistical studies required a careful balancing of the individual's interest in personal privacy with society's need for knowledge. First, unlike the other uses of records addressed in this memorandum, research and statistical activities generally do not lead to an immediate or direct benefit for the individual subject. While the researcher may ask for the individual's participation or for information about him, society as a whole, rather than the individual, is the ultimate beneficiary.

Second, research and statistical studies rely heavily on the voluntary cooperation of research subjects in providing accurate information. As an inducement to candor, research subjects are generally given a promise of confidentiality or anonymity before being asked to provide information, especially for research studies related to controversial issues, such as drug abuse, sexual behavior, or abortion. However, as discussed below, the law does not protect these records when they are sought by a government agency.

Finally, research studies increasingly rely upon the availability of records and data bases maintained by third-party record keepers, both government and non-government. No law establishes protection for the individual whose records are disclosed for such a purpose.

Current Law and Practice

Current Federal law protects from compelled disclosure a limited number of statistical and research records collected for specific purposes. HEW, for example, may authorize researchers engaged in mental health or alcohol or drug abuse research to withhold names or identifying characteristics of data subjects, and this immunity covers them in any Federal, state, or local civil, criminal, administrative, legislative or other proceeding. (42 U.S.C. 4582) Such protections do not, however, exist in most cases where research is conducted using records with confidential information on the record subject. Moreover, some Federal statutes are now drawn to facilitate the exchange of data so that it may be used for both administrative and research purposes, thereby eliminating redundant collection. (44 U.S.C. 3501-5311)

In gaining access to personal records, researchers generally give assurances that the information will be held in confidence, and ordinarily strive to preserve that confidentiality. However, even the most well-meaning researcher may be forced to disclose information under court order or subpoena, lest he pay the personal consequences of violating that order. And increasingly both private and public organizations are seeking access to "confidential" research data.

Discussion

A policy addressing the use of personal records for research and statistical studies should set out two fundamental standards: first, the rules governing when a researcher may have access to personal records that were not collected for research purposes; and second, the rules governing when records collected for research purposes may be used for non-research purposes.

Area of Agreement

Access by researchers to personal records collected for non-research purposes.

The Commission's judgment, strongly supported by the agencies, is that for socially desirable research and statistical studies to continue, laws are required permitting, and regulating, access by researchers to medical, educational, and social service records (the records most often used in these studies). It is agreed that researchers must at times be allowed access to these records in individually identifiable form even without the direct consent or knowledge of the subject individual. It is also agreed that, to protect the record subject, the institution maintaining the records should conduct a responsible review of research protocol and enter into a written agreement with the researchers assuring that the privacy of the individual will be protected. These laws would apply to records generated with Federal funds for use by the Federal government.

Area of Disagreement

Access to research and statistical records for non-research purposes.

The Privacy Commission recommended that there be a clearly delineated boundary between the use of personal

information for research and statistical purposes and its use for administrative or other purposes. This principle of "functional separation" would mean that, aside from instances where the health and safety of the individual and society are involved, research and statistical records (however collected) could never be used in any way to make a decision about or take an action against the subject individual.

For example, according to the principle of functional separation, personal records collected for research on drug abuse could not be disclosed to a narcotics officer for criminal prosecution or used administratively to determine support payments while the individual was undergoing withdrawal therapy.

The Commission did not, however, recommend that research and statistical records be totally immune from disclosure subject to court order. The principle of "functional separation" would allow for court ordered disclosures needed: 1) to prevent imminent physical injury; 2) where there is an alleged violation of law by the researcher or institution; or 3) for audit purposes. The principle would apply to research and statistical records generated with Federal funds for use by the Federal government.

The question for decision, therefore, is:

1. Should there be a Federal statute establishing a policy of "functional separation," such that no personal information collected or maintained for a research or statistical purpose may be used or disclosed in individually identifiable form so as to allow any decision, or to facilitate the taking of any action, directly affecting the individual to whom the record pertains?

Pro:

This, the Commission's proposal, is supported with some modification by DHEW, the Department of Labor, the National Archives and Records Service, and the Veterans Administration, and is also strongly supported by the research community. All believe that a standard of confidentiality, such as is established with "functional separation," is essential to ensure the continuing integrity of research and statistical studies. They fear that research subjects will not voluntarily participate in these

studies in the future if no strict legal standard of confidentiality exists protecting them from use of the information to affect them adversely, particularly since it is society as a whole, not the individual research subject, that benefits from his participation. To allow an exception for access to these records for law enforcement purposes, however legitimate, would, they argue, effectively undermine the entire approach.

Con:

The law enforcement agencies, including the Departments of Treasury and Justice, oppose the Commission's proposal in that the belief that data collected by a government agency for use in research and statistical studies should be available to that agency for other purposes needed to accomplish its mission, and to any second agency which has the legal authority and the need to collect the information. The particular concern is for successful law enforcement. Moreover, these agencies, as well as a number of others, believe that it will be very difficult and perhaps costly to classify records for either "research and statistical purposes" or for "administrative use" when they are frequently used for both purposes.

Decision:

_____Yes, there should be such a policy of "functional separation" for research and statistical records.

_____No, there should not be such a policy.

D. Coverage of the Wiretap Statute

The statute that prohibits most wiretapping defines wiretapping as the "aural" acquisition of communication. This definition arguably does not cover the digital transmission of conversations or data.

Some argue that this definition should be revised so that digital transmissions are clearly covered. However, as noted in Section I.B above, this memorandum deals only with information privacy, excluding matters such as wiretapping and other forms of electronic surveillance to the extent they do not involve the information practices of a record keeper. The Privacy Commission did not address the issue of wiretapping and most agencies have not yet taken positions. However, the Department of Justice is now preparing draft amendments to the wiretapping statute to remove the present ambiguities.

## VI. Allocation of Federal Privacy Responsibilities

### Issue

A variety of personal privacy protections have been created by Federal law, and this memorandum has discussed possible areas of new privacy protections. In addition, there are questions of whether the Federal government should undertake certain administrative functions relating to the protection of privacy in the Federal and non-Federal sectors, as well as what organization should be responsible for carrying out each of the functions deemed necessary.

### Discussion

The Privacy Commission concluded that the existing Federal administrative structure for overseeing Federal agencies' collection and disclosure of information and for implementing the Privacy Act is inadequate. As discussed earlier, each agency is responsible for its own implementation of Privacy Act responsibilities. OMB is tasked in the Act with providing oversight and guidance regarding the Act's implementation, although it has no authority to enforce any guidance or interpretation it may provide. In practice, the agencies generally follow OMB's guidance, absent some compelling agency interest to the contrary. The Commission found a consensus among the agencies that OMB has been less active and less effective in the privacy area than it might have been, although this is perhaps understandable considering the restrictions placed on it. OMB has been limited in its role by personnel restraints and by Congress' rejection of a centralized enforcement approach in the Privacy Act.

The Commission found that some agencies regard privacy concerns either as an afterthought or as an impediment to their substantive program missions. Within an agency, the unit with privacy responsibility is often under pressure to decide favorably to, and in accordance with, the program needs of the agency. There have been cases of differing interpretations of the Act's requirements within agencies which have no central privacy coordinator. Moreover, there is no office which monitors, reviews, and coordinates Privacy Act compliance at the Federal level for all of the agencies.

The Commission also observed that there are some issues that individual agencies cannot, and in certain cases

should not, resolve on their own. The most obvious of these is the question of whether a particular type of record-keeping system should exist at all; another is whether particular transfers of records among agencies are desirable; and still another is whether certain types of information should be considered public information. The Commission believed that such questions require independent policy judgments, often on a government-wide rather than an agency-by-agency basis, and thus should be addressed by a unit with government-wide privacy oversight authority.

Of equal importance, the pressures to fulfill primary program functions tend to lead agencies to design information systems with regard only to program objectives and not privacy or similar social concerns. Such a narrow focus for system design and development often short-changes the rights and interests of individual citizens. In addition, failure to consider questions such as privacy, and incorporate appropriate protections, at the design stage of a system can lead to substantial waste; development of systems has been stopped after considerable investment when Congress and others have discovered a lack of consideration for individual rights in the system design. Internal agency processes which could help alleviate part of this problem were identified in Part IV. In addition, a credible, politically accountable central oversight unit would enable the Federal government to take effective and fiscally prudent advantage of new information technologies.

Additionally, there are a number of Federal laws covering portions of the non-Federal sector which affect personal privacy. Some, like the Family Educational Rights and Privacy Act, give a single agency (HEW) enforcement responsibility. Others, like the Fair Credit Reporting Act, the Fair Credit Billing Act, and the Equal Credit Opportunity Act, place primary enforcement responsibility with one agency, the FTC, but give authority to other agencies on a selective basis (e.g., the Comptroller of the Currency has enforcement authority for national banks and the Federal Reserve Board for member non-national banks). Some statutes, like the Equal Credit Opportunity Act, give rulemaking authority to one agency (FRB) and enforcement authority to another (FTC). While most of the laws allow an individual to take legal action to protect himself, no agency has overall responsibility to develop privacy policy or monitor and evaluate activity outside the Federal sector. If a privacy policy is adopted for the private sector,

the variety and number of Federal regulatory and enforcement agencies which would be involved suggested to the Commission the need for a central Federal entity which could assist and direct the development of a uniform approach.

Three additional considerations common to both Federal and non-Federal privacy policy combined with those previously discussed to lead the Privacy Commission to urge creation of a new and independent Federal organization. First, the Commission, itself limited to a two-year life by statute, saw a need for some body which would be able to respond on a continuing basis to the unforeseen consequences of the growth of information technology and to suggest any needed executive and legislative action. Second, the absence of a forum for continued study and evolution of new policy responses--whether or not technology pushed the issue to the fore--was viewed as a serious weakness of the current system. Finally, the Commission strongly believed that there was a need for a central organization to which an individual could turn for non-regulatory and non-enforcement assistance, whether his problem was caused by a Federal agency or by a private organization. The entity could advise the individual, but enforcement authority would remain in existing agencies.

The response to the Commission proposal for the creation of an independent entity with privacy responsibilities has received a mixed reception in the Congress. In some quarters, the concept is endorsed, either as a separate organization or as part of a larger agency dedicated to individual rights concerns. The response of a few critical committees (particularly in the House) has been, at best, unenthusiastic.

A majority of the executive agencies oppose the idea of an independent agency. Most agencies do, however, agree that there are additional administrative functions dealing with privacy which should be undertaken by the Executive Branch. There was, though, no agreement on either the specific functions or the agency or agencies which should discharge them.

Issues for Decision

Two basic questions require decision. First, what additional privacy-related functions should be undertaken by the Executive Branch? Second, what organization(s) should be responsible for carrying out those functions?

## Proposed Functions

1. Should oversight of Federal agencies' records management practices for personal information (including implementation of the Privacy Act; collection of information; and design, development, and operation of record systems) be substantially strengthened by designating a high-level unit with authority to issue binding decisions, regulations, or interpretations implementing the Privacy Act?

These decisions, regulations, and interpretations would deal not only with procedural matters but also with the determination of what information must be made available to individuals or the public at large in the context of the privacy exemption to the Freedom of Information Act, although in no instance would it be directed or suggested that information about an individual be withheld from individuals.

This proposal is supported by the Privacy Commission's findings on the ineffectiveness of current oversight of the Privacy Act and the need to increase agency accountability to solve problems which cannot or should not be resolved by a single agency and to ensure more effective application of the Act. Such a central oversight function would address the need for early and adequate review of proposals for the development of new systems to assure that privacy and other social implications have been fully accomodated in the system design. (Additional supporting arguments for this proposal have been made earlier in this section and in Section IV.A).

Many agencies oppose establishing a centralized Privacy Act oversight function, although some support the creation of an effective dispute-settling mechanism for inter-agency conflicts. Arguments against establishing such a function begin with the observation that it is a major departure from the concept of agency autonomy in the original Privacy Act. Concern is also expressed that sufficient experience has not yet been acquired to validate the need for this new function.

A danger of overlap of responsibility between an organization exercising this new authority and existing agencies is also foreseen. It is pointed out that creation of such general oversight responsibility would weaken the responsibility and consequent diligence of Federal agencies.

Decision:

_____ Create such authority.

_____ No.

2. (a) Should the Federal government monitor and evaluate information privacy practices in the non-Federal sector, including voluntary compliance by non-Federal sector organizations with Administration policy?

(b) Should a government function be designated to provide expert advice and assistance to the President and the agencies on privacy matters, including the privacy implications of proposed statutes and regulations, new or revised record systems, and agencies' information collection practices?

(c) Should authority and resources be designated for conducting ongoing studies of privacy questions, particularly in regard to the consequences of the growth of information technologies, in both the public and private sectors?

The Congress and most observers have concluded that privacy is a "permanent" public policy issue which will not be resolved by this or any other single initiative. Continuing advances in computer and telecommunications technology alone will precipitate changes in the concentrations and flows of personal information in American society which will result in privacy protection problems. The Federal government will be under increasing pressure to attend to the privacy issue, and to do so will require consistent and continuing policy responses. Thus far, principal difficulty in developing a coherent Federal privacy policy has been the lack of a stable body with expertise and authority to advise the President and Congress. In the past five years, three organizations with responsibility for considering privacy problems have been created and then disbanded: The HEW Advisory Committee; the Domestic Council Committee on the Right to Privacy; and the Privacy Commission. In addition, there have been numerous other, more narrowly focused, Federal activities. Expense and duplication of effort has been great. Policy development would be more cost-

effective, and arguably better, if permanent and adequately staffed responsibility in this area were given to one organization.

Furthermore, as the Privacy Commission and other observers have noted, oversight of agency activity to ensure it conforms with existing policies is not enough. Most oversight, for example, is necessarily triggered by agency requests for funding to develop or procure new systems. The pace of technological change, particularly the rapid decrease in hardware costs and systems development, will soon make such an oversight process obsolete. Sophisticated computer and telecommunications systems will no longer cost millions or even hundreds of thousands of dollars, and agencies will be able to meet their computer and telecommunications needs for a price which will make budget-triggered review impracticable. Additionally, the proliferation of low-cost home and office computer systems, and their consequent interconnection to larger systems and data bases, raises a host of privacy-related questions, even the outlines of which are still unclear. In order to effectively develop and apply privacy policy, responsibility needs to be established for the consideration of new technological developments and the policy responses which will be needed.

Most agencies support subsection (a) of this proposal, noting that such responsibility can logically be shared by agencies with existing mandates in the appropriate private sector area. For example, the Department of Labor believes that it can perform an important function in connection with employment records. Additionally, private sector organizations favor some form of monitoring of their voluntary compliance so that they can be assured that their efforts will be considered and evaluated before any legislative efforts are undertaken. Agencies generally concur with subsections (b) and (c).

International considerations also support this proposal. The United States is unlikely, in the near future, to establish a privacy-related regulatory authority for the public and private sectors, as is the trend in other countries. Representatives of the international community recognize this, but they still would prefer one focal point to which they could take their concerns on privacy-related issues.

Decision:

__✓__ Establish these functions.

_____ No.

3. Should authority be established for a government entity to participate in Federal administrative proceedings of other agencies materially affecting personal privacy, including the presentation of testimony and other evidence but not including any right to seek, or participate in, judicial review of agency actions?

Such a function would help ensure continued and systematic attention to privacy concerns throughout the regulatory and decision-making structure of government. In addition, it would give a legitimate and presumably effective voice to concerns which are currently usually ignored.

Most executive agencies and corporate interests oppose the grant of this authority. They believe it would only burden an already overburdened process. In addition, they feel that the responsibility for ensuring proper attention to privacy concerns should remain with each agency. Finally, it is noted that with increased access to administrative proceedings by a wide variety of public interest groups such authority may not be necessary.

Decision:

_____ Yes, there should be an agency with authority to fulfill this responsibility.

_____ No.

4. Should individuals be able to obtain government assistance with regard to privacy-related problems of concern to them, particularly regarding the information collection practices of specific agencies or organizations?

Such a "complaint" function would not provide any authority to correct problems. It would simply establish a single place to which individuals could bring their concerns or to which they could go in order to discover the appropriate channels for redress of grievances. In addition, this function would permit the organization exercising it to bring systematic patterns of complaint to the proper forum for attention, be it an agency, the President, or Congress.

A priority for this unit would be to consider the propriety of information which Federal agencies collect. The

Privacy Act of 1974, while admonishing agencies to maintain only such information "as is relevant and necessary," provided no opportunity for challenging the general collection practices of an agency. The Act permits only limited challenge, through its access and correction provisions. In addition, this challenge mechanism operates after the fact; there is no way for an individual to dispute collection before it occurs. Finally, even if an individual successfully challenges the existence of a specific item of information in his record, the removal of that item from his record would have no effect on either the continued collection of such items by an agency or their continued existence in other persons' records.

Most of the executive departments endorse the idea of providing a mechanism for challenge, but few wish to see any new authority at this time. They prefer to rely on their own judgments, and they feel that individuals should bring their grievances directly to the concerned agency. (Such a "mechanism" need not be a governmental unit. It could also be a self-executing statute giving an individual rights of the sort provided in the Privacy or Fair Credit Reporting Acts, although this is not being proposed at this time.) In addition, OMB already has some authority to review the propriety of agency collection practices under Section 3506 of Title 44, although admittedly, Section 3506 incorporates no standards of review, nor does it facilitate individual challenges to agency collection.

Private sector organizations oppose this because they believe that it would encourage unnecessary complaints and dissatisfaction to be expressed. In addition, this proposal would probably demand considerable resources of staff and money without a tangible benefit to the government in return. Finally, it might frustrate individuals who would find the unit unable to actually solve their problems.

Decision:

_____ Establish such a mechanism.

_____ No.

## Assignment of Privacy Functions

5. To what organization(s) should the above new functions be delegated?

If any new, or augmented, functions are created, the question remains of where they should be lodged. The functions established could be alloted among existing agencies, or to a new organization.

The Privacy Commission recommended a new entity within the Executive Branch. The Commission argued that no existing agency has a mandate to carry out privacy functions. It concluded that a new organization is needed because existing agencies have competing interests and responsibilities which would make it very difficult for them to carry out the proposed functions even-handedly and because some of the functions to be performed call for a consideration of competing interests between agencies.

Most agencies do not believe such a new organization is necessary. They contend that existing agencies could perform both private and public sector functions. OMB currently exercises responsibility for the Privacy Act and its role could be continued and extended. The Commerce Department's National Telecommunications and Information Administration (NTIA) is currently the focal point for Adminstration studies and programs in the area of information and communications privacy, and other agencies, such as the Departments of Labor and HEW, are also currently working in the privacy area.

___ Create a new privacy organization, with appropriate resources.

___ Divide functions between existing agencies, with appropriate resources, as follows:

Oversight of Federal Agencies (Issue 1):

✓ Commerce (NTIA)
___ GSA
___ Justice
___ OMB
___ (other)

Development of privacy policy, including advice to the President, agencies, and Congress (no regulatory authority) (Issues 2, 3, and 4):

✓ Commerce (NTIA)
____ Justice
____ OMB
____ (other)

Appendix: Compilation of Decisions

## I. Introduction

### G. The Elements of a Privacy Policy

#### 8. Implementation

Area of Agreement

Except as otherwise indicated in the remainder of this memorandum, the basic implementation strategy proposed by the Commission has been assumed for the purposes of drafting this memorandum. While the agencies have not spoken directly to the issue of implementation strategy, except as indicated below, their responses to the specific recommendations of the Commission suggest agreement with the Commission's implementation strategy.

II. Non-Federal Records

B. Consumer Credit Industry

Areas of Agreement

There is agreement among the Commission and most agencies responding that, in the area of consumer credit, Federal law should require:

a) that credit grantors notify individuals at the time of application for credit of their collection and disclosure practices, and follow that notice;

b) that individuals have the right to automatically be given the reasons for an adverse credit decision; and, upon request, to see and copy the specific item(s) of information used in making that decision;

c) that credit grantors promptly send any corrections of inaccurate, untimely, or incomplete information to credit bureaus, debt collection agencies, or authorization services to whom the inaccurate information has previously been disclosed;

d) that credit authorization services be covered by the requirements placed upon credit grantors and credit bureaus (including the requirements placed on consumer reporting agencies by the Fair Credit Reporting Act), except for the requirement to propagate corrections (in (c) above);

e) a legally enforceable expectation of confidentiality (as defined in Section I.G.7); and

f) enforcement by:

(i) an individual right of action, and

(ii) the FTC or bank regulatory agencies for repeated or systematic violations.

Areas of Disagreement

1. Should an individual have a right to see and copy at any time all reasonably retrieveable records

about him held by a credit grantor, not just the items of information that have been used to make an adverse decision (as set forth in 1(b) above).

Decision:

_____ Yes, the individual should have a right of access to all credit records upon request.

_____ No, an individual right of access to credit records should be limited to those records that have been used to make an adverse decision about him.

2. Should an individual have access to credit records about him maintained but not prepared by the institution from which he seeks the records, e.g. credit reports in the hands of a credit grantor?

Decision:

_____ Yes, an individual should have a right of access to credit records about him maintained but not generated by the institution from which he seeks the records.

_____ No, an individual's right of access to credit records should be limited to those records generated by the institution from which he seeks the records.

3 Should there be a mechanism for the individual to challenge the relevance and propriety of information collected or used by credit grantors?

Decision:

_____ Yes, there should be governmental mechanisms for the individual to challenge the relevance and propriety of information collected or used by credit grantors.

_____ No, such mechanisms should not be created.

4. Should Federal law require that a credit grantor have reasonable procedures to ensure the accuracy, timeliness, and completeness of the personal information it collects, maintains and discloses?

Decision:

_____ Federal law should require a credit grantor to have reasonable procedures to ensure the accuracy, timeliness, and completeness of the information it collects, maintains, and discloses.

_____ Federal law should require that a credit-card issuer adopt reasonable procedures to ensure that the information it discloses to an independent authorization service is accurate at the time of disclosure.

_____ Adopt no new "reasonable procedures" requirement in consumer credit.

C. Commercial Credit Industry

Issues for Decision

With regard to the records about individuals created and maintained by commercial credit grantors and commercial reporting services, the Privacy Commission recommended that Federal law provide:

1) An individual right, upon request, to see, correct, and amend information about him maintained by a commercial credit reporting service;

2) An individual right to be notified, upon request, by a commercial credit grantor who has used a commercial credit report containing personal information on the individual to make an adverse credit decision, of the identity of the commercial credit reporting service that made the report; and

3) enforcement by:

   a) an individual right of action, and

   b) the Federal Trade Commission for repeated or systematic violations.

1. Should the recommendations of the Privacy Commission (listed above) for the personal records created and maintained by commercial credit grantors and reporting services be adopted in Federal law?

Decision:

_____ Yes, the Privacy Commission recommendations (as listed above) should be adopted in Federal law (using, to the extent possible, the regulations implementing the Equal Credit Opportunity Act and otherwise through a new Federal statute).

_____ No, the Privacy Commission recommendations should not be implemented through legislation, but should be suggested as voluntary standards with legislation to follow in the event of non-compliance.

_____ No, take no action.

2. Should Federal law require that commercial reporting services have reasonable procedures to assure the accuracy, timeliness, and completeness of information pertaining to individuals included in reports produced by them?

Decision:

_____ Yes, Federal law should require that commercial reporting services have reasonable procedures to assure the accuracy of information pertaining to individuals included in reports produced by them.

_____ No, such requirements should not be imposed.

D. Depository Institutions

Areas of Agreement

There is agreement among the Privacy Commission, the Department of Commerce, and significant segments of the banking industry that, with regard to depository institutions, Federal law should require:

a) that depository institutions notify applicants of their collection and disclosure practices, and follow that notice;

b) that depository institutions promptly notify independent check-guarantee and check authorization services of corrections of erroneous information previously reported to them;

c) that check-guarantee and check-authorization services be subject to the provisions of the Fair Credit Reporting Act;

d) a legally enforceable expectation of confidentiality (as defined in Section I.G.7.); and

e) enforcement by:

(i) an individual right of action, and

(ii) the FTC or other depository institution regulatory agencies for repeated or systematic violations.

Areas of Disagreement

1. Should an individual have the right to be given the specific reasons for an adverse depository decision and to be informed of the specific item(s) of information used in making that decision?

ecision:

____ Yes, require disclosure of the reasons for an adverse depository decision and, upon request, the items of information used in making the decision.

____ No.

2. Should an individual have a right to see and copy at any time all reasonably retrievable records about him held by a depository, not just the items of information used to make an adverse decision?

Decision:

_____ Yes, the individual should have a right of access to all depository records upon request.

_____ No, an individual right of access to depository records should be limited to those records that have been used to make an adverse decision about him.

E. Insurance Industry

Areas of Agreement

Although there is disagreement about how privacy protection in the insurance industry be implemented, the Commission, the Department of Commerce, and some insurance companies, particularly in the life and health areas, agree that substantive protections should include:

a) a requirement that insurance institutions notify applicants of their collection and disclosure practices, and follow that notice;

b) the right for an individual to challenge the accuracy of those insurance records to which he has access (as defined below);

c) a requirement that the record keeper send any corrections it makes of inaccurate information to:

   i) anyone designated by the individual who has received the inaccurate information within the preceeding two years;

   ii) any support organization which regularly receives such information; and

   iii) any support organization which furnished the inaccurate information;

d) a prohibition on pretext interviews, (an interview in which an investigator: (1) pretends to be someone he is not; (2) pretends to represent someone he does not; or (3) misrepresents the purpose of the interview);

e) the right for an individual to be given the reason(s) and item(s) of information used in an adverse insurance decision;

f) the right for an individual not to be denied insurance based solely on the fact that he previously has been denied insurance; and

g) a legally enforceable expectation of confidentiality (as defined in Section I.G.7).

Areas of Disagreement

1. Should the privacy protections applicable to the insurance industry be required by Federal law?

Decision:

_____ Yes, privacy protections applicable to the insurance industry should be required by Federal law.

_____ No, regulation of the insurance industry's privacy practices should be left to the states.

2. Should an individual have a right to see and copy the records about him maintained by an insurance institution, including information used by an insurer in making an underwriting decision?

Decision:

_____ Yes, an individual should be able to see and copy the records about him maintained by an insurance institution, including the records used in making underwriting decisions.

_____ No, an individual should have no such right of access.

3. Should an individual's right to see and copy the records maintained by an insurance institution include first-party claims records?

Decision:

_____ Yes, an individual should be able to see and copy first-party claims records maintained by an insurance institution.

_____ No, an individual should not have a statutory right to see and copy first-party claims records, independent of court action.

4. Should an individual's right of access to his insurance records in the hands of an insurance company or support organization include access to information prepared by another institutional source, e.g., a consumer investigative report maintained by an insurance company?

Decision:

_____ Yes, an individual's right of access to his insurance records should include access to information originating with another institutional source.

_____ No, information originating with another institutional source should be excluded from an individual's right of access to his records in the hands of a recipient record keeper.

5. Should there be a mechanism for the individual to challenge the relevance and propriety of information collected or used by an insurer or insurance support organization?

Decision:

_____ Create a Federal governmental mechanism (using the Federal Insurance Administrator or other Federal entity), and urge the states to create state governmental mechanisms, for the individual to challenge the relevance and propriety of information collected and used by insurance institutions.

_____ Urge the states to create governmental mechanisms for the individual to challenge the relevance and propriety of information collected and used by insurance institutions.

_____ No such mechanisms should be created.

6. Should Federal law require insurance institutions to adopt reasonable procedures to ensure the accuracy, timeliness, and completeness of the information it collects, maintains, or discloses about an individual?

Decision:

_____ Yes, insurance institutions should be required to adopt reasonable procedures to ensure the accuracy, timeliness, and completeness of the information they collect, maintain, or disclose about an individual.

_____ No, there should be no such statutory requirement.

F. Employment Records

Areas of Agreement

There is agreement among the Privacy Commission, the Department of Labor, and private employers that privacy protection in private sector employment should include:

a) an employer's notice to his employees of the collection and disclosure practices;

b) an opportunity for the individual to see and copy the records maintained by his employer;

c) an opportunity for the individual to correct and amend his records;

d) a limitation on disclosure to that contained in the notice;

e) a prohibition on pretext interviews (an interview in which an investigator: (1)pretends to be someone he is not; (2)pretends to represent someone he does not; or (3)misrepresents the purpose of the interview); and

f) that for the job-related records which an employer maintains, the above principles should be endorsed by the government but made voluntary, not mandatory, on the part of the employer.

Areas of Disagreement

There is a need for decision in the employment area on the following two questions, which go beyond the above noted areas of concensus and would implement by statute some of these measures.

Should there be a Federal law granting employees the right to see and copy the personal records which their employer maintains about them?

Decision:

_____ Yes, there should be a Federal law granting employees the right to see and copy the personnel records their employer maintains about them.

_____ No, employee access to employment records should be sought through voluntary action on the part of employers.

2. Should there be a legally enforceable expectation of confidentiality (as defined in Section I.G.7) for employment records?

Decision:

_____ Yes, there should be a legally enforceable expectation of confidentiality for employment records.

_____ No, employers should limit their disclosures of information on employees through voluntary action.

3. Should the Department of Labor develop a voluntary code of conduct for those privacy measures recommended for voluntary adoption in employment, and monitor compliance with that code?

Decision:

_____ Yes, the Department of Labor should develop a voluntary privacy code for employers and monitor their compliance.

_____ Yes, the Department of Labor should develop a voluntary privacy code for employers, but should not monitor their compliance.

_____ No, the Department of Labor should not develop such a code.

G. Medical Records

Areas of Agreement

The Commission, the responding agencies, and the medical community agree that a Federal law to establish privacy protections for medical records is needed. Such protections would include:

a) the right for an individual to have direct access to the medical records about him (i.e., to see and copy those records), except when the medical professional responsible for the record believes direct access to it might harm the patient, in which case access should be permitted through a designated intermediary;

b) the right for an individual to challenge the accuracy of his medical records;

c) a legally enforceable expectation of confidentiality (as defined in Section I.G.7); and

d) authorizing the Secretary of HEW to issue implementing regulations, and encouraging the states to adopt similar legislation governing medical record keepers not subject to Federal law.

Issue for Decision

The Department of Health, Education, and Welfare has drafted legislation implementing the above principles of privacy protection for medical records, and this proposed legislation has been circulated for agency comment through OMB's legislative clearance process. Agencies that have not received copies should contact OMB. Any agency concerns may be resolved through the OMB process, or, if necessary, should be raised for inclusion in this Presidential Review Process.

H. Education Records

Areas of Agreement

The Commission and the Department of Health, Education, and Welfare agree that, beyond the current provisions of FERPA, there is a need for:

a) greater student involvement in developing privacy policies to comply with FERPA, and greater community involvement in the case of public school systems; and

b) an explicit statutory right of action for the individual against any educational institution which fails to comply with FERPA to the detriment of a student or parent.

Areas of Disagreement

1. Should FERPA be extended to cover applicants for admission to schools and colleges, and to educational testing and data-assembly services?

Decision:

_____ yes, extend FERPA to cover applicants for admission, and educational testing and data-assembly services

_____ no, do not extend FERPA to applicants for admission, and educational testing and data-assembly services.

2. Should FERPA be amended to provide that the student or his parent may not waive his right to see and copy letters of recommendation?

Decision:

_____ Yes, FERPA should be amended to provide that the student or his parent may not waive his right to see and copy letters of recommendation.

_____ No, FERPA should not be so amended.

3. Should Federal law (FERPA) be amended to require educational institutions to adopt reasonable procedures to ensure the accuracy, timeliness, and completeness of the records they collect and maintain?

Decision:

_____ Yes, FERPA should be amended to require educational institutions to adopt reasonable procedures to ensure the accuracy, timeliness, and completeness of the records they collect and maintain.

_____ No.

I. Public Assistance and Social Service Records

Areas of Agreement

The Commission and the responding agencies agree that privacy protection for public assistance and social service records should include:

a) a requirement that applicants be notified of public assistance and social service programs' collection and disclosure practices, and that the notice be followed;

b) the right for an individual to have access to his records, except for:

i) records being used in an ongoing investigation of suspected violations of law by the individual;

ii) medical information, in certain situations as defined in Section II.G, above; and

iii) the identity of sources of information who request confidentiality, and then only when the source's information is not the sole basis for an adverse decision;

c) the right of an individual to challenge the accuracy of his records; and

d) a legally enforceable expectation of confidentiality (as defined in Section I.G.7).

Areas of Disagreement

1. Should an applicant for public assistance and social service programs be able to prevent an agency from obtaining and using information from sources other than himself (i.e., a collateral source) without his consent by requiring the agency to notify him any time it desires to contact a collateral source and allowing him to withdraw his application if he does not want the source to be contacted?

Decision:

_____ Yes, an applicant should be able to prevent an agency from contacting collateral sources without his consent by withdrawing his application.

_____ No, an applicant should not be able to prevent an agency from contacting collateral sources.

2. Should privacy protections in the area of public assistance and social service programs be implemented by a Federal law setting forth general standards and requiring states to enact specific legislation within two legislative sessions? (The alternative is for these protections be embodied in Federal law and required of states as a condition of receiving Federal funds.)

Decision:

_____ Adopt the Commission proposal of general Federal standards and required specific state legislation.

_____ Adopt the DHEW proposal of specific Federal requirements being a condition of receiving Federal funds.

3. Should Federal law require states to provide by statute that public assistance and social service agencies must have reasonable procedures to ensure the accuracy, timeliness, completeness, and relevance of the records they maintain and disclose?

Decision:

_____ Yes, Federal law should require states to provide by statute that public assistance and social service agencies must have reasonable procedures to ensure the accuracy, timeliness, completeness, and relevance of the records they maintain and disclose.

_____ No.

J. Telephone Toll Records

Issue for Decision

1. Should the individual have an expectation of confidentiality (as defined in Section I.G.7) for telephone toll records?

Decision:

_____ Yes, an expectation of confidentiality should be created for telephone toll records.

_____ No, an expectation of confidentiality should not be created for telephone toll records.

## III. Government Access to Personal Records Held by Third Parties

### Areas of Agreement

There is general agreement throughout government that new legal protections for personal privacy need to be established when government seeks records about individuals held by certain private sector record keepers. Specific agreement exists as follows about what some of the elements of such protection should be.

1. Notice to an Individual of Government Access to His Records

2. Protections Would Only Apply When the Individual to Whom the Records Pertain is the Subject of an Investigation

3. Protections Only for Natural Persons

4. Exclusion of Search Warrants

### Areas of Disagreement

A. Nature and Substance of Protections Where an Individual is Deemed to Have an Expectation of Confidentiality

This group of issues defines the process that will be used for access to the records in which individuals are to be given an expectation of confidentiality. This expectation of confidentiality has been defined in section I.G.7, and the kinds of records to which it applies have been identified in Part II.

1. Should government access to confidential records always be through compulsory process?

(Page 102)

Decision:

_____ 1. Require the use of compulsory process for all government access requests for those types of records in which the individual has an expectation of confidentiality.

✓ 2. Permit agencies or their components that do not have authority to issue subpoenas or administrative summons to use a formal written request procedure for those types of records in which the individual has an expectation of confidentiality.

Collateral Decision:

Irrelevant if Decision 2 above is adopted.

Seek legislative authority for administrative summons powers for _____.

2. What should be the nature of the judicial standard which can be employed by an individual in order to make the government justify its access request?

(Page 104)

Decision:

_____ Adopt Commission proposal: burden on the government to establish specific relevance of its request first; "reasonable cause" standard.

✓ Adopt Justice/Treasury proposal: burden on individual to come forward and establish factual basis for questioning propriety of government request; "legitimate law enforcement purpose" standard.

_____ Adopt compromise: burden on government of initially coming forward; "reasonable relationship of record sought to an ongoing investigation of a violation of law" as sole standard.

3. What should be the exceptions to the notice and challenge rights?

(Page 108)

Decision:

_____ Adopt the Commission notice and challenge proposal.

__✓__ Adopt the Justice/Treasury notice and challenge proposal.

_____ Adopt the compromise set forth above.

4. Should judicial subpoena in the course of litigation be covered?

(Page 78)

Decision:

_____ Apply the access proposals to judicial subpoena in the course of litigation.

__✓__ Exempt judicial subpoena from access proposals in the course of litigation.

5. Should the standards for the issuance of, and use of information obtained by, administrative summons be reformed?

(Page 73)

The Commission recommended tightening the procedures for the issuance of administrative summons and imposing limitations on the use of personal information obtained by administrative summons. Specifically, the Commission recommended that Federal law provide that:

a) an administrative summons may be used only to inspect records required by law to be maintained by the record keeper;

b) the information acquired with the administrative summons may be used only for purposes of the investigation or enforcement action which justified acquisition of the information; and

c) an administrative summons must be issued by a supervisory official and not a field agent.

Decision:

_____ Adopt Commission issuance and use recommendations.

__✓__ Retain present law without change.

6. Should the standards protecting the secrecy of information obtained by a grand jury which assure protections for individuals under investigation be reformed? (Page 115)

The Commission's proposed grand jury reforms would require that personal information obtained through use of a grand jury subpoena:

a) be returned and actually presented to the grand jury;

b) be employed only for a criminal prosecution where the grand jury issuing the subpoena issued a presentment or indictment;

c) be destroyed or returned to the record keeper where no indictment or presentment is issued (except to the extent that the information has become part of the official minutes of the grand jury);

d) not be copied or kept apart from the sealed records of the grand jury; and

e) be protected by stringent penalties for improper use or disclosure outside the grand jury.

Decision:

_____ Adopt Commission grand jury recommendations.

__✓__ Adopt Justice/Treasury approach and retain present law without change.

B. Extension of parts of government access recommendations to records where an individual does not have an expectation of confidentiality and to the collection practices of state and local governments.

7.A Should government requests for private sector records other than those covered by an expectation of confidentiality (as decided in Part II) be documented by a "paper trail" to create greater accountability?

(Page [illegible])

Decision:

____ Letterhead request

____ Compulsory process

__✓__ No paper trail

7.B Should requests by Federal agencies for personal records held by state and local governments be subject to some restrictions?

(Page [illegible])

Decision:

____ Letterhead request

____ Compulsory process

__✓__ No paper trail

8. Should state and local government agencies be restricted in their information collection practices?

(Page [illegible])

Decision:

____ Apply all access provisions directly by Federal law to all Federal, state, and local government agencies.

__✓__ Apply access provisions directly only to Federal agencies; but expressly permit, by statute, states to adopt new access processes which incorporate at least the minimum protections for Federal agencies.

____ Apply access provisions only to Federal agencies; exempt the states from both the particular access provisions for Federal agencies and the provisions of the legally enforceable expectation of confidentiality (as defined in Section I.G.7 and decided in Part II) which prohibit informal access by government agencies.

C. Compulsory Reporting Requirements

9. Should there be reform of compulsory record-keeping and reporting statutes?

(Page 124)

Decision:

_____ Adopt the Commission position.

_____ Adopt the HEW position: endorse substance of Commission position but implement specific standards by regulation.

✓ Adopt the Justice position: reject limitation on uses and redisclosures and implement remaining substance of Commission position by regulation.

IV. Federal Record-Keeping

A. The Privacy Act of 1974

Issues for Decision

1. Should the Administration endorse revision of the Privacy Act?

(Page 152)

Decision:

_____ Endorse Privacy Commission recommendations to fundamentally revise and strengthen the Act.

_____ Endorse concept of fundamental revision of Act in 1979-80 Congress with goal of strengthening Act while minimizing agency burden; assign staff to review issues and develop positions.

__✓__ Defer fundamental changes in Act until there is more experience under it; plan tentatively to seek legislation in 1981.

2. Should the applicable provisions of the Privacy Act apply to records generated by Federal funds, for use by the Federal government (i.e., should recipients of discretionary Federal grants be included under the Act)?

(Page [illegible])

Decision:

_____ Extend provisions of Act to recipients of discretionary Federal grants administratively.

__✓__ Do not extend Act.

3. Should the "routine use" provision of the Act be substantially strengthened?

(Page 136)

Decision:

_____ Revise the "routine use" provision along lines recommended by the Commission.

_____ Accept concept of revising "routine use" standard; instruct staff to develop alternative to Commission's approach.

__✓__ Take no action (i.e., retain current "routine use" standard).

4. Should a position be created within each agency to oversee implementation of the Privacy Act?
(Page 137)

Decision:

__✓__ Adopt Privacy Commission proposal to create an agency position to oversee implementation of the Privacy Act.

_____ Take no action.

5. Should the processes of internal agency oversight in the development of new systems for the use and storage of personal records be reformed?
(Page 138)

Decision: (Any number of those options may be selected)

__✓__ Assign oversight and review responsibilities to the designated agency official.

_____ Establish guidelines on the responsibility, training, and appointment of system managers.

_____ Adopt earlier trigger mechanism for external oversight.

B. Federal Provision of Data-Processing and Telecommunications Services: Electronic Funds Transfer

Areas of Agreement

There is agreement that privacy protections for EFT should include, in addition to the provisions generally applicable to depository institutions, the following:

1. Individually identifiable account information generated in the provisions of EFT services should be retained only in the account records of the financial institution and other parties to a transaction, except that it may be retained by the EFT service provider to the extent, and for the limited period of time, that such information is essential to fulfill the operational requirements of the service provider;

2. Procedures should be established so that an individual can promptly correct inaccuracies in transactions or account records generated by an EFT system, so as to provide protections for EFT systems comparable to these provided by the Fair Credit Billing Act for credit-card systems.

3. With respect to government-operated systems: (Note: provisions 3(a) and (b) below are recommendations of the National Commission on Electronic Fund Transfers, and have been considered only by the 12 Federal agencies represented on that Commission, rather than by all the agencies involved in this review process.)

   a) Any government agency providing EFT services should follow privacy rules and procedures that are at least as restrictive as those of private sector EFT system operators; and

b) Access by other government agencies to records of EFT transactions in the temporary possession of a government EFT service provider should be governed by rules and procedures that are at least as restrictive as those for access to EFT records maintained by private sector financial institutions.

Issue for Decision

1. Should the Federal government withdraw from, or restrict its operations of, EFT services for the private sector?

(Page 146)

Decision:

✓ Do not limit government operation of EFT for the private sector at this time. * OF

____ Provide that no government entity be allowed to own, operate, or otherwise manage any part of an electronic payments mechanism that involves transactions among private parties.

____ Allow government operation of automated clearinghouses (ACHs), but not, at present or in the foreseeable future, of point-of-sale switching and clearing facilities, except for the provision of net settlement among depository institutions.

STAT * Per [redacted] OF disagrees with the implication that this option should be of limited duration, hence deletion of "at this time".

V. Other Issues

A. The Use of Truth Verification Devices in Employment

Issue for Decision

1. Should Federal law prohibit the use of polygraph and other truth verification devices in employment?

(see 150)

Decision:

_____ Yes, prohibit the use of polygraph and other truth verification devices in employment.

__✓__ Take no position.

_____ Oppose Federal legislation.

B. Standard Personal Identifier

Areas of Agreement

There is agreement among the Commission and the agencies on the following points concerning privacy protections for a Standard Personal Identifier:

a) the Federal Government should do nothing to foster the development of a Standard Personal Identifier until it has addressed the underlying issue, which is controlling the disclosure and exchange of recorded information; and

b) the limits currently placed by Section 7 should not be increased.

Areas of Disagreement

1. Should Executive Order 9397 (a 1943 order directing Federal agencies to use the Social Security Account Number when establishing a new system of permanent account numbers) be amended so that Federal agencies may not, as of January 1, 1977, rely on it as legal authority by which to create new demands for the disclosure of an individual's Social Security Account Number (SSAN)?

(Page 155)

Decision:

_____ Yes, amend E.O. 9397 so that Federal agencies may not, as of January 1, 1977, rely on it as legal authority by which to create new demands for the disclosure of an individual's Social Security Account Number.

__✓__ No, do not amend E.O. 9397.

C. Research and Statistical Studies

Area of Agreement

Access by researchers to personal records collected for non-research purposes.

The Commission's judgment, strongly supported by the agencies, is that for socially desirable research and statistical studies to continue, laws are required permitting, and regulating, access by researchers to medical, educational, and social service records (the records most often used in these studies). It is agreed that researchers must at times be allowed access to these records in individually identifiable form even without the direct consent or knowledge of the subject individual. It is also agreed that, to protect the record subject, the institution maintaining the records should conduct a responsible review of research protocol and enter into a written agreement with the researchers assuring that the privacy of the individual will be protected. These laws would apply to records generated with Federal funds for use by the Federal government.

Area of Disagreement

1. Should there be a Federal statute establishing a policy of "functional separation," such that no personal information collected or maintained for a research or statistical purpose may be used or disclosed in individually identifiable form so as to allow any decision, or to facilitate the taking of any action, directly affecting the individual to whom the record pertains?

(Page 159)

Decision:

____ Yes, there should be such a policy of "functional separation" for research and statistical records.

✓ No, there should not be such a policy.

VI. Allocation of Federal Privacy Responsibilities

Issues for Decision

Proposed Functions

1. Should oversight of Federal agencies' records management practices for personal information (including implementation of the Privacy Act; collection of information; and design, development, and operation of record systems) be substantially strengthened by designating a high-level unit with authority to issue binding decisions, regulations, or interpretations implementing the Privacy Act?

(Page 165)

Decision:

____ Create such authority.

_✓_ No.

2. (a) Should the Federal government monitor and evaluate information privacy practices in the non-Federal sector, including voluntary compliance by non-Federal sector organizations with Administration policy?

(b) Should a government function be designated to provide expert advice and assistance to the President and the agencies on privacy matters, including the privacy implications of proposed statutes and regulations, new or revised record systems, and agencies' information collection practices?

(c) Should authority and resources be designated for conducting ongoing studies of privacy questions, particularly in regard to the consequences of the growth of information technologies, in both the public and private sectors?

Page 166

Decision:

__✓__ Establish these functions.

_____ No.

3. Should authority be established for a government entity to participate in Federal administrative proceedings of other agencies materially affecting personal privacy, including the presentation of testimony and other evidence but not including any right to seek, or participate in, judicial review of agency actions?

(page 160)

Decision:

_____ Yes, there should be an agency with authority to fulfill this responsibility.

__✓__ No.

4. Should individuals be able to obtain government assistance with regard to privacy-related problems of concern to them, particularly regarding the information collection practices of specific agencies or organizations?

(page 161)

Decision:

_____ Establish such a mechanism.

__✓__ No.

Assignment of Privacy Functions

5. To what organization(s) should the above new functions be delegated?

_____ Create a new privacy organization, with appropriate resources.

__✓__ Divide functions between existing agencies, with appropriate resources, as follows:

Oversight of Federal Agencies (Issue 1):

__✓__ Commerce (NTIA)
_____ GSA
_____ Justice
_____ OMB
_____ (other)

Development of privacy policy, including advice to the President, agencies, and Congress (no regulatory authority) (Issues 2, 3, and 4):

__✓__ Commerce (NTIA)
_____ Justice
_____ OMB
_____ (other)

Executive Registry
78-8401/3

This is the draft Response Memorandum on Privacy. Because it is a preliminary draft, it should be circulated only to those in each agency who need to see it. Its contents should not be discussed outside the agency.